Health Technol. (2017) 7:469–487
DOI 10.1007/s12553-017-0203-5

ORIGINAL PAPER

The Aadhaar: "Evil" Embodied as Law

Tathagata Satpathy[1]

Received: 7 May 2017 / Accepted: 2 June 2017 / Published online: 17 July 2017

Abstract India is known the world over for many wondrous details; history of human origins, languages, mathematics, medicine, music, foods, culture, scenic beauty, landmarks, diversity of peoples, climates, contrasts and above all, spirituality. More recently, however, India, and the distressing privacy annulling actions on the sub-continent have become the chief discussion point among those in the world who are alarmed over the ways in which personal privacy is being encroached upon by moneyed interests of all variety, and by those governments who are willing to collude with them, under false pretenses. In a nation with nearly 1.4 billion people, one readily identified as the world's largest democracy, forces are now at work, arbitrarily, autocratically, undemocratically, and unconstitutionally deploying, what has come to be known as the world's largest biometric national ID program (scans and captures iris, fingerprints and facial inputs into a government database), called *The Aadhaar. The Aadhaar,* initially sold to the tax-payer as a program only to exist per volunteer citizen participation, has speedily, and in the span of less than 2 years, gone from being that volunteer participation program, to a "you must enroll" program, intent on siphoning a citizen's most personal information into government custody. More importantly, the government, against initial Supreme Court ruling, is now actively pushing for the widespread adoption of *the Aadhaar* into every segment of the Indian Society, without any constitutional reading, deliberation or ruling. As a member of the national parliament, and as the only opposing voice to the implementation of *the Aadhaar,* in a chamber of 545 members, the author aims to candidly introduce the reader to the leading issues that are enabling the Central government and moneyed interests to collude, and to suppress democratic processes to ramrod *the Aadhaar* legislation through the parliament as a 'money bill,' and what this Indian program and experience could herald.

Keywords Aadhaar · India · Privacy · Data protection · Surveillance · GDPR · Tathagata Satpathy · BPO

1 Introduction

The debate around Privacy in India has been mainstreamed primarily due to the introduction and implementation of a national biometric identification program called *"the Aadhaar"* (termed 'basis', when loosely translated to English). This program was launched by a Central government agency based in New Delhi, called the Unique Identification Authority of India (UIDAI).[1] The agency mandate is to issue *the Aadhaar*, or a set of unique identifying numbers (12 digit) to each individual Indian citizen, which will be foundationally reinforced by highly sensitive citizen biometric information. The proponents of this program are primarily certain corporate heads who are linked to the Information Technology business on one side, and important bureaucrats of the Central Government on the other. Politicians of all hues have been coaxed and convinced to accord extreme importance to the implementation of *Aadhaar*, while the Supreme Court of India seems totally out of touch, being indecisive, and unable

This article is part of the Topical collection on *Privacy and Security of Medical Information*

✉ Tathagata Satpathy
tatzaudi@yahoo.com

[1] Parliament of The Republic of India, Government of The Republic of India, 2 Feroze Shah Road, New Delhi 110 001, India

[1] Unique Identification Authority of India, Official Website - https://uidai.gov.in/

to deliver any judgement - in any matter coming up before it regarding *the Aadhaar*, and all too importantly, matters related to privacy issues.

The crisis that the Supreme Court of India seems to be suffering from, and the consequential crisis that the court is now inflicting upon the Indian population, is perhaps succinctly presented by Pratap Bhanu Mehta, the Scholar President of Centre for Policy Research (India), in a prominent national newspaper article thus: "*[f]irst, the court has created a credibility crisis for itself. Its mendacious evasions on the issue of privacy rights emanating from Aadhaar have eroded its credibility. In a context where the Supreme Court has found time to take over entire private bodies like the BCCI (Board of Cricket Control of India) and run them, the idea that it did not have time to conduct hearings since October 2015 on an issue of such vital importance is frankly scandalous.*"[2]

"Something is rotten in the state of Denmark."[3] This is perhaps the best way to pose the nature of problem associated with *the Aadhaar* Program to the reader. However, to utilize that well-known declaration in Shakespeare's Hamlet to present, that in relation to *the Aadhaar*, there is presently a mishandling of the Indian body politic, which, according to this author, borders on negligence encouraged by a fast flowing river of intellectual and moral (and perhaps even a political) corruption - could perhaps be interpreted being either imperious, or inconsiderate. But, assurances are presented to the reader that it is neither, rather, the reference is being used fairly and justifiably to introduce the reader to the nature and texture of the *evil*, that which is *the Aadhaar*. In all, this article shall seek to present certain important multidimensional perspectives, as to why, the largest national biometric identification program in the world, called *the Aadhaar*, now being illegitimately deployed, should, and in no uncertain terms - be terminated. In Hamlet, "Heaven will direct it,"[4] said the exclaimant Horatio; where, as in India's case, no Heaven shall be able to direct good fortunes for the nation from the clutches of this *evil* known as *the Aadhaar*. Only a motivated group of well-informed Indians may be able to liberate themselves and their fellow citizens from a central government imposed digital self-enslavement; speedily taking shape in a country widely identified as the World's largest democracy.

2 The concept of evil, in relation to the launch of "*The Aadhaar*" program

The author has offered comments within this article, from a basis that *the Aadhaar* Program and the associated services are *"evil."* In order to better explain why a reference to the term *"evil"* is being made, in relation to *the Aadhaar*, and to better represent the author's views regarding parliamentary responsibilities – especially given the social implications of the way *the Aadhaar* program is being deployed and used, a proper examination of the term *"evil"* must first be briefly made. The term *"evil"* is used cavalierly and liberally in polity, internationally. In fact, the concept of *evil* can be clouding for many, if not most [1]. Then why has this author chosen to centralize his objections to *the Aadhaar*, with the use of this term? The answer is fairly simple; in that, if the meaning of the term *"evil"* as it was being referred to in this article could be provided, and made clear, then the reader could suitably grasp how the author, a Citizen of India, and a parliamentarian would opposed *the Aadhaar* scheme from the very beginning.

In "The Rhetorical Impact of Evil on Public Policy," Jonathan Anderson has, in this author's view, managed to condense a good span of Social Science's view on the proper use of the word *"evil",* and in the manner this author has intended. Anderson explains that references to the word *"evil"* can be, both, represented and understood in terms of *"... an intense exploitative connection with another person, or a total disconnection with the humanity of others."* Anderson has further qualified that the reference to *"evil,"* is normally *"... limited to human actions toward other humans, separating people designated as evil - from the rest of humanity"* and that *"[t]he rhetorical reference to evil, represents an example of 'sensemaking,' where such a reference then places the otherwise incomprehensible, within an understandable framework"* [1].

Many widely incomprehensible points and fellow aspects regarding *the Aadhaar* exist. The discussion of each and every incomprehensible point, and their associated aspects are beyond the scope of this writing. However, it is sufficient to say that in the view of this author, many of the specificities associated with *the Aadhaar*, are *manufactured realities*.[5] For those

[2] Pratap Bhanu Mehta; Supreme Test', The Indian Express, 6 May 2017 - http://indianexpress.com/article/opinion/columns/supreme-test-4642608/

[3] The Tragedy of Hamlet, Prince of Denmark, William Shakespeare Act 1, Scene 4, The Complete Works of William Shakespeare, MIT, Boston, MA, 2017.

[4] *Ibid*

[5] Hugo award winning novelist Philip K. Dick once said the following, with respect to "manufactured realities," which is an apt explanation and representation of the term, one that is better than any that can be presented in a dictionary, especially given the context. Dick said, *"Today we live in a society in which spurious realities are manufactured by the media, by governments, by big corporations, by religious groups, political groups... So I ask, in my writing, what is real? Because unceasingly we are bombarded with pseudo-realities manufactured by very sophisticated people using very sophisticated electronic mechanisms. I do not distrust their motives; I distrust their power. They have a lot of it. And it is an astonishing power: that of creating whole universes, universes of the mind. I ought to know. I do the same thing." – Philip K. Dick,* et al.*, in: "I hope I shall Arrive Soon", Doubleday, New York, New York, 1985.*

not familiar with the term: *manufactured realities,* one prominent example of it is the phrase "Axis of Evil",[6] – introduced to the world by the former US President George W. Bush. Representations produced since and surrounding an industrialized publicizing of that term after 9/11 – have in fact, widely exposed how *realities can be manufactured* [2].

The very advancement of *the Aadhaar* program is invigorated in fact, by *manufactured realities,* packaged neatly with prosaicism, a certain banality, if you must, by the program's inceptors. The charms and spells of this prosaicism, have at the core, promises of massive national savings to be realized from such things as the curbing of corruption at a transactional level – one between an Indian Citizen and his/her government, or various government agents. Most programs, or action emphases that are sold to government power structures as being a 'life or death need,'[7] are very often stuffed with such neatly packaged prosaicisms.

Elizabeth Minnich [3], has carefully unwrapped for us her attentive examinations of such packaged prosaicisms, which she has identified as, *"the evil of banality, the profound dangers of [that emanate from] clichéd thoughtlessness".*[8] In a very illuminating way, Minnich's finding could perhaps best explain the national-level cultural and political action motivations behind *the Aadhaar*. Minnich candidly characterizes humanity's general tendency to unleash profound dangers through thoughtlessness, in the following manner. She says:

> …. when systems go bad, when the extraordinary becomes ordinary, it does not take a Hitler, an Idi Amin, a Jeffrey Dahmer, a Charles Manson. It just takes a practiced conventionality, a cliche'd conscience, emotional conformity, susceptibility to small-scale bribery by salary, goods, and/or status, a sense of isolation, and distrust of the reliability of others that works against taking a differing public stand. **It just takes, that is, much of what in better times keeps a society provided with reliable and ambitious workers, status-anxious consumers, polite neighbors, agreeable team players, and citizens who make no waves: an ability to go along thoughtlessly, to play the game.**[9]

To take a differing public stand, this author-parliamentarian would like to present to the reader a scholarly view from someone internal to India, from one who has been researching *the Aadhaar* for the many implications of its introduction into Indian society. Prof. R. Ramakumar, the Dean of the School of Development Studies at the Tata Institute of Social Sciences has fundamentally epitomized the problem that this author has objected to from the very start. It is, as Prof. R Ramakumar has said: the "States were not consulted [4]"! He goes further and has characterized the way *the Aadhaar* program was ramrodded through Parliament as, "an attempt to destroy the federal fabric of the Indian constitution."[10]

To introduce such a large public program into the Indian society, and one especially that will adversely affect nearly 1.4 billion people; to legitimize its existence under one 'stated' objective; to provide public funds for its bureaucratized implementation, and then to implement it under quite another set of objectives – all carrying with it - as an almost daily mission metamorphosis with alarming social implications and deciding to foist all of this upon a largely unsuspecting population, thoroughly unaware of the social implications, is, plainly *"evil".*

The near absence of oppositional (tr)action and voices in the Parliament against *the Aadhaar* is perhaps explainable, if we reflect further with Minnich. By reason, she shows the following reality to otherwise aggrieved minds, who may still acrimoniously glimpse at the veracity of the proposition. She says:

> I fear that the banality of evil is itself becoming a banality, a cliche´, in ways that gut its force. In general, now, 'the banality of evil' means that 'ordinary people,' and not just Grand Villains, are capable of doing excessive harm. That is not wrong, but it is utterly inadequate, sliding as it does toward a notion that goes even further than collective responsibility toward once again swamping individual responsibility. **If everyone is guilty, then no one bears actual responsibility.**
>
> **But collective responsibility and guilt together create an appealing position. The combination gives us company, lots of it, and that is a fine way to avoid those dark nights of the soul in which we take**

[6] Frances Romero; "George W. Bush and the Axis of Evil", Time, 25 January 2011

[7] *"UID – 'Aadhaar' was touted out as a 'transformational' initiative – one that would change the face of India, make it the most digitised nation in the world, with the biggest data base of demographic information anywhere and so forth."* – Mathew Thomas; "How does govt justify 'Aadhaar' when its foundation has crashed?" The Deccan Herald, 20 December, 2011 http://www.deccanherald.com/content/212980/how-does-govt-justify-aadhaar.html **and** *"We need to remove everybody's curtains so we can look through the terrorists' windows," .... When you argue back, security and privacy are presented as an incompatible binary. "Well, you have nothing to hide, do you? Don't you want to stop terrorists?"* –Amelia Tait; "Technology and tragedy: How the government uses terrorism to justify surveillance: Can we trust that new security measures are anti-terrorist and not anti-democracy?", NewStatesman, 4 April 2017 http://www.newstatesman.com/science-tech/internet/2017/04/technology-and-tragedy-how-government-uses-terrorism-justify

[8] The "*profound dangers of clichéd thoughtlessness"* in this case relates to ones inability to resist a succumbing to the empty promises of savings to be made on behalf of the national treasury.

[9] Minnich, *supra,* ref. [3] [bolding and underlining do not exist in the original]

[10] Prof. R. Ramakumar, cited Prime Minister Narendra Modi as having said: "… it's actually a problem of federalism in India and hence a problem of democracy that the government is not discussing these matter with state governments at all." *Supra* ref. [4]

account of our lives. But moving in close, we cannot sustain that step outside, the already-cliche'd 'we're all capable . . . ' in order to think afresh.[11]

3 A brief sanity check

The aforementioned sketch does not represent any judgment by this author, rather, it should only serve to position properly an important point, which in this case is: that a malicious social-engineering[12] program, such as *the Aadhaar*[13] is now being implemented on a massive scale in this densely populated country, and is virtually going unnoticed or undernoticed (at best)[14] in India.

To underscore the aforementioned point relating to *the Aadhaar* program being deployed without generating any great loathing at all by most Indian citizens, the reader's attention is drawn to a statement recently made by the Attorney General of India, before the Supreme Court on 2 May 2017, where the Attorney General presented before the esteemed court that 'Citizens (of India) should not expect to have, and in fact do not have, absolute right over their own bodies'.[15] These words were presented in relation to the Supreme Court's query to whether there exists a requirement to compel Indian Citizens to avail themselves before government, or government sanctioned entities, to provide biometric information such as, Iris scans, Fingerprints and other type of scans as may be provisioned for, through incremental legislation - including DNA data – which could be made mandatory for obtaining *the Aadhaar* card. Only a few newspapers published any extract at all from the submission made by the chief law enforcement officer of the Government of India before the Supreme Court, while the electronic media completely ignored this very important notable.

Today, in the twenty-first century, privacy has not only been challenged by private interests such a online services, merchants and data-brokers, but, through *the Aadhaar* program, the Indian State itself has launched a major challenge – one, that seems to annihilate right to privacy completely.

4 Programmatic background

The Aadhaar program was launched in 2009, and was purely voluntary till 2016, when the Government of India passed a legislation in the Parliament[16]giving the program legal status. Since that time the government has been aggressively pushing its implementation across the country, and beyond the bounds of original program intent and allowances. Through Mission-Creep,[17] the Government of India now claims that it has enrolled 99% of the national population into *the Aadhaar* program,[18] which de facto would make *the Aadhaar*, the largest biometric identification system in the world.

In simple words, *the Aadhaar* project aims to assign to every citizen a unique 12 digit number which will be foundationally connected to their biometric attributes (Fingerprints, photograph, iris and other scans). This Unique ID (UID) will be stored in a single server, which would have gateways that allow authentication of that person.[19] The earliest of propositions before the government put forward the grand idea that when a citizen avails himself/herself to collect government assigned welfare benefits, or any other government provided service, *the Aadhaar* program will be used to authenticate the recipient as being the correct party - rightly authorized to receive government benefits. Since 2009 however, the Government has been[20] claiming that *the Aadhaar* program would prevent informational leakages and curb corruption, which happens presently at a large scale on the ground during distribution[21] of state largesse.

The *manufactured reality*[22] as it related to *the Aadhaar* program, and its original purpose of merely providing a voluntary "yes/no" authentication mechanism - has dramatically changed in the last year. The born again *Aadhaar* scheme is dangerous

[11] Minnich, *supra* ref. [3] "bolding ["and underlining"] do not exist in the original"

[12] The "Social-Engineering" inference - as it refers to the Aadhaar program is strictly provided here in terms of Karl Popper's reference to the same, as: "…a method which, …may easily lead to an intolerable increase in human suffering." – Karl R. Popper; "The Open Society and Its Enemies - The Spell of Plato" [Vol. I], Butler & Tanner Ltd., London, 1947

[13] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.- https://uidai.gov.in/images/the_aadhaar_act_2016.pdf

[14] This reference does not imply in any way that the Aadhaar program implementation is being carried out under the cover of darkness, instead, the reference is to suggest that the public is unaware of the many large scale social implications of Aadhaar program's implementation, and their participation within it.

[15] Amit Anand Choudhary; "Citizens don't have absolute right over their bodies: Government", Times of India, 3 May 2017 - http://timesofindia.indiatimes.com/india/citizens-dont-have-absolute-right-over-their-bodies-government/articleshow/58486260.cms

[16] The Aadhaar, *supra* note 13

[17] Oxford Living Dictionaries defines "Mission-Creep" as, "A gradual shift in objectives during the course of a [……] campaign, often resulting in an unplanned long-term commitment." [https://en.oxforddictionaries.com/definition/mission_creep]

[18] Unique Identity Covers to Over 99 Percent Adult Residents of India', Press Information Bureau of India, 27 January 2017 – http://pib.nic.in/newsite/PrintRelease.aspx?relid=157709

[19] Central ID Repository of India (CIDR) - https://authportal.uidai.gov.in/developer

[20] Press Trust of India (PTI); "Aadhaar law will ensure DBT reaches genuine beneficiaries: Arun Jaitley", Economic Times, 15 July 2016 - http://economictimes.indiatimes.com/news/economy/policy/aadhaar-law-will-ensure-dbt-reaches-genuine-beneficiaries-arun-jaitley/articleshow/53230263.cms

[21] Saurabh Kumar; "How Aadhaar plugs leakages in PDS and LPG subsidy transfer", The Mint, 14 August 2016 - http://www.livemint.com/Politics/ZRbi2x5IaxrDhHU65m2gOK/How-Aadhaar-plugs-leakages-in-PDS-and-LPG-subsidy-transfer.html

[22] Matthew D. Matsaganis and J. Gregory Payne; *supra* ref. [2]

because it now allows third parties, other than the Government of India, to use this citizen database for their own purposes, whatever they may be. A surreptitious concept to be more intrusive into people's lives and their details - called e-KYC ("Know Your Customer") was introduced through regulations in September[23] of 2016. This KYC allows private companies to acquire Indian government issued licenses that would subsequently permit them to access *the Aadhaar* server for drawing-out information on registered citizens. Such access is now being used to issue SIM cards by mobile phone companies,[24] to verify new recruits,[25] obtain banking services[26] and even the issuances of driving licenses.[27] Present day reports claim that this system will now be implemented in airports to verify passengers before they fly,[28] and to compel taxpayers to quote their *Aadhaar* number when filing returns and paying taxes.[29]

A citizen is required to produce an *Aadhaar* card and number, to buy an electric vehicle under the Faster Adoption and Manufacturing of (Hybrid and) Electrical Vehicles in India (FAME- India) Scheme, as do those students, who wish to appear for the National Entrance Eligibility Test (NEET). Such drastic changes to the original policy imply that *the Aadhaar* is not designated for limited uses anymore – particularly not just for availing government doles, or subsidies or even curtailing corruption.

The Delhi State government recently pushed the use of *the Aadhaar* program even further, by making the unique identification number a compulsory requirement for children who desire to seek admission into any school.[30] Why is the Indian public being an agreeable and consenting lot - in the deployment of this *evil* program? For this, the reader should be presented with at least a broader familiarization to the present day constitution of Indian society.

This familiarization shall aim to at least introduce the fundamental reasons as to why the vibrant youth populations of India - digitally very enabled - are yet, far less privacy conscious than their Western counterparts. Additionally, this author shall attempt also to introduce briefly, the deeply entrenched cultural drivers that power and willingly sanction the vast penetration of *the Aadhaar* program into the multi-layered structure of the Indian society. Within the article's scope and other limitations, these examinations, at the root, aim to introduce the reader to reasons for which the general population has, more or less proposed that they are blameless in *the Aadhaar*'s launch, and remain largely unperturbed at present by the manic *Aadhaar* push undertaken by the Government of India.

5 Cultural background – A contributor to privacy insensitivity

Primarily, privacy is an obscure concept to comprehend for the majority of Indians, due to historical and socio-economic conditions. Interestingly in most Indian languages, no word exists for 'privacy'. The recent lingua franca in texts on the subject of privacy have per force, preferred to use words that resemble and frame aspects of 'secrecy' more. Naturally, since privacy is not a semantic equivalent of secrecy, linguistically, none should synonymize them. The concept of privacy, in the form that it is vigorously considered in the West is mostly an extra-terrestrial proposition to many Indians. So much so that they do not even bother to try and understand what privacy truly could mean to them, and how the absence of privacy could be detrimental to them in a globalized state of existence, both economically and socially.

On the sub-continent, historically, people have had large families and have mostly lived together. Inter-generational family households have been more the norm where parents with multiple daughters, sons, daughters in law, and grand children often live under one roof. One supporting reason for this inter-generational existence is linked to economics [5–7] first, where a huge family was/is incapable of owning or hiring a bigger home, and secondly, for a need for greater social cohesion.[31] Mostly, however, family members

[23] e-KYC service, Government of India, UIDAI Official website - https://uidai.gov.in/authentication/aadhaar-financial-inclusion/aadhaar-e-kyc.html

[24] Reliance Jio, SIM card activation in 5 min, Jio Care website - https://jiocare.net/jio-ekyc-sim-activation-process-using-aadhaar-card/

[25] Yuthika Bhargava; "App to verify domestic helps, employees using Aadhaar", The Hindu, 6 March 2016 - http://www.thehindu.com/news/cities/Delhi/now-app-to-verify-domestic-helps-employees-using-aadhaar/article8319500.ece

[26] Ivan Mehta; "IT Department Makes Aadhaar Linkage Mandatory For Bank Accounts Opened In A Certain Period", Huffington Post, 12 April 2017 - http://www.huffingtonpost.in/2017/04/12/it-department-makes-aadhar-mandatory-for-bank-accounts-opened-in_a_22036324/

[27] Dash, Dipak K; "Aadhaar to be mandatory for driving licence," The Times of India, 26 March 2017 http://timesofindia.indiatimes.com/india/aadhaar-to-be-mandatory-for-driving-licence/articleshow/57834023.cms

[28] "Aadhaar may soon become mandatory to board planes for domestic flights", India today, 2 May 2017 http://indiatoday.intoday.in/technology/story/aadhaar-may-soon-become-mandatory-to-board-plane-for-domestic-flights/1/920919.html

[29] Ameet Patel; "The Backdoor Entry Of Aadhaar Into Income Tax Law And Its Implications," BloombergQuintOpinion/Bloomberg, 27 March 2017 https://www.bloombergquint.com/opinion/2017/03/25/the-backdoor-entry-of-aadhaar-into-income-tax-law-and-its-implications

[30] 'Delhi government schools are turning away children who don't have Aadhaar', Scroll.in, 11 April 2017 https://scroll.in/newsrepublic/834245?s=cm

[31] "building shared values and communities of interpretation, reducing disparities in wealth and income, and generally enabling people to have a sense that they are engaged in a common enterprise, facing shared challenges and that they are members of the same community" – Rosell et al. [8] and "People in joint families learn lessons of patience, tolerance, cooperation and adjustment. They also learn what it means to take collective responsibility. When young people live with senior members of the family from the time they are born, they grow up appreciating, admiring and loving them. They also learn to adjust because they realize that as younger people, they have the flexibility of adjusting and changing whereas older people often get caught up in patterns of functioning." –Chadha [9]

appreciate the closeness among members. Under such a setting, when guests and friends are able to visit and discussions of a personal nature are to be conducted, the only available space for such an activity is often one's own bedroom. Many a times, newly-wed couples have found that it a necessity to share a room with siblings.

As a means of comparatively explaining, consider that on the average, there are 4.91 people per Indian household [10], while there are only 2.64 people on the average per US household [11]. Such a closed circuit upbringing in India has served to not just instill, but to also cement certain inexperience, or unworldliness toward the more global concept of privacy, and the larger world's societal norms involving privacy. The indigenous cultural foundations have also made it possible for many in India to outwardly project among fellow Indians themselves a complete disregard to and for 'the need to respect the individual's space'. In other words, *our national mindset has been tuned* towards accepting that citizens have no privacy. This should come as no great surprise, when in fact, it has been discovered that people's views related to "privacy" are generally a byproduct developed from those traditional views and the cultural values they hold and actively exhibit in daily existence.[32] More generally, it is safe to say that the internal Indian struggle to make progress in the modern world, in all aspects of society, especially in the sphere of economy, is made more cumbersome by deeply entrenched cultural norms and traditions. To make matters more complex, there are those that argue that a blanket privacy law in India akin to that of the EU will not work, and would not be best suited for India, given India's cultural differences with the West [15].

This parliamentarian has a vastly different view than his compatriots in this regard. There must be a harmonization of Privacy related personal viewpoints, social attitudes, and national frameworks for privacy protections, defence and repatriation mechanisms for Indian citizens, despite the vastly differentiated political and socio-economic nature of Indian States, and respective administrative frameworks, if India is to be a strong economic member of the international community of goods and services producers. Such foundations are equally important and necessary also to enable Indians to thrive as global consumers as well.

5.1 Language & Inter-Generational Tensions as a contributor to privacy insensitivity

The deep tensions and upheavals that the Indian society is experiencing, among which, one is the nature of India's collective capability to sufficiently and correctly advance lawful and enforceable personal privacy protections, particularly in terms of Privacy, To understand why the acknowledge condition is so, the following information must be well comprehended.

India is home to Christianity, Judaism, Islam, Buddhism, Jainism, Sikhism, Zoroastrianism, and to the world's oldest continuous faith – Hinduism (Hindooism), among other faith sets and sub-sets, which are practiced today.[33] The country boasts approximately 780 living languages [16] among the nearly 1.4 billion people[34] who now call the Sub-Continent, home. The Sub-Continent parades many peoples, and their high contrasted cultural and socio-economic existence; these contrasts are made intimate through the wide human geography[35] of the country.

With this sea of population and cultural dynamism, India is eager to be informationally connected. India's younger population is hungry for faster & more efficient economic progress too. Migration from rural & semi-urban areas to urban areas has exposed them to many opportunities on a global scale that was beyond their reach previously. Rural-to-urban and urban-to-urban migration flows have increased, especially among men [17]. The exposure to urban opportunities has granted affluence to many, while many more have continued to remain disadvantaged. An analysis by the World Bank Group has revealed considerable occupational mobility across generations. Over 40% of the children of unskilled worker parents were holding other occupations at the time of the analysis. Furthermore, about 36% of the children of farmers were working as skilled or semiskilled workers, or as white-collar workers. Lastly, occupational mobility across generations has also increased over time.[36] These indicators show a creation of more affluence among migrants, general upward mobility, and more participation in the national economy. Moreover, as the Confederation of Indian Industry notes, Indian consumers are rapidly advancing towards adopting technology, and towards the end of 2015, for instance, India beat the United States to become the second largest market for smartphones, after China.[37] As we observe these brief views of pockets of population experiencing enrichment, taking a closer look at the larger

[32] See: [12–14]

[33] "By 2050, India to have world's largest populations of Hindus and Muslims - Religious Composition of India," Pew Research Center, Washington, DC, April 20, 2015 http://www.pewresearch.org/fact-tank/2015/04/21/by-2050-india-to-have-worlds-largest-populations-of-hindus-and-muslims/ft_15-04-17_indiashare/

[34] **1,340,708,984** as of Friday, May 22, 2017, based on the latest United Nations estimates. Source: "worldOmeters", at: http://www.worldometers.info/world-population/india-population/

[35] Human Geography "is the study of the different ways in which human societies develop and operate in relation to their physical environment", Definition of "Human Geography," The Cambridge Advanced Learner's Dictionary & Thesaurus, Cambridge University Press, 2017 https://dictionary.cambridge.org/us/dictionary/english/human-geography [Human Geography studies concentrate on such things as cultural, social, developmental, economic, political, and even health aspects of populations in relation to their environments, and the many associated attributes]

[36] *Ibid*

[37] "e-Commerce in India A Game Changer for the Economy", Deloitte Touche Tohmatsu India LLP & Confederation of Indian Industry, Delhi, India April 2016

national picture relating to migration and affluence will tell a different story; a story of social, economic, psychological strife and political exclusion (Fig. 1).

The relationship of aforementioned factors to the lack of personal privacy awareness, individual and collective privacy practices, play a significant role in defining the texture of privacy shapes and privacy conditions in the Indian society. UCLA Historian Vinay Lal has managed to describe what the societal upheavals (in the way they are occurring) and the tension-ridden economic 'push-pull' influences have done to Indians. Lal says that India's drive towards a "culture of modernity," influenced by "indigenous and foreign corporate interests," and "international finance organizations such as the IMF and the World Bank," have stimulated the rise of "gross materialism of middle-class Indians" and has "eroded the image [of India] as a land of sublime spirituality [18]."

Yet, in the middle of all 'socio-econo-politico' parboiling of the Indian society, in direct relation to privacy, and in the age of Facebook, Twitter, Snapchat, Uber, Data-Brokers and *the Aadhaar*, we must scrutinize that India's Internet User population has jumped from nearly 5.6 million (.5% population penetration) in 2000, to nearly 470 million in 2016 (34.8% population penetration).[38] The number of Internet Users in India is slated to surpass 500 million by the end of 2017. Of this, nearly 400 million will be mobile users.[39] We must be reminded that, more and more, the connected mobile populations in India are the young, affluent, and upwardly mobile members of the census, who are largely 'privacy unconscious.' For example, Indian mobile Internet users under 25 years of age were carefully reviewed for a University of Maryland study, whereupon it was discovered, and with only negligible differences between sexes, that men and women commonly used their devices for entertainment purposes, negotiation of independence from parents, forming friendships with the opposite sex, and for private communication, and private needs [19]. While salient to those who will independently observe with their "eyes wide open,"[40] the important point to be considered here with respect to the growing number of 'privacy unconscious' young users of India are the following.

Older generations of Indians are no different than the older populations in other countries. The older generations

Fig. 1 Connected Youth of India. Source: Public Domain

are not adept at navigating new and available technologies, those emerging technologies, and, or their effects upon themselves and society. On the other hand, the younger generations of Indians, while eager and adept at the use of technologies are vastly different from their counterparts in other countries, for they are not guided by those critical attributes, which could have been inter-generationally passed-on through Cultural Transmission.[41] As Bisin and Verdier have indicated from a theoretical and empirical perspective that, "*"Cultural transmission"* arguably plays an important role in the determination of many fundamental preference traits, like *discounting, risk aversion* and *altruism*. It plays a central role in the formation of cultural traits and norms, like attitudes towards the family, towards fertility practices, and in the job market."[42] The absence of *cultural transmission* pathways that impart critical technology use related knowledge and the multiple social implications of technology use - disadvantage the youth in India. Adjoiningly, one should take note that Social Media platforms like Facebook and Twitter are more recent advents, and in terms of India's past, cultural history, technology adoptions, and technocratic evolution, contiguously considering also, that previous generations possess neither knowledge nor skills, transmittable through modalities of *cultural transmission*, that would inherently benefit India's technologically savvy middle-class with respect to privacy.

As a result, generations of Indians are now standing at an ontological intersection, wondering what privacy is, what is it that they themselves could do to ensure it, and assure it for the future. They are also wondering, more importantly, why, since, in relation to *the Aadhaar*, the Indian government is bent on embracing and championing a scheme that fundamentally weakens the constitutional rights of the Indian peoples. In fact, robs them of it (See Fig. 2), despite the fact that India is a signatory to the

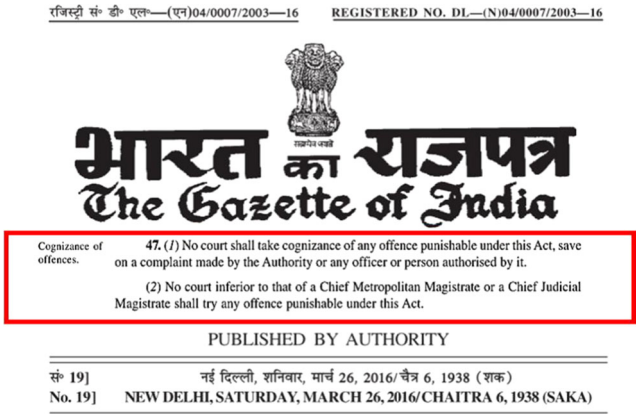
[38] India Internet Users: 462,124,989, Internet Live Stats [Elaboration of data by International Telecommunication Union (ITU), World Bank, and United Nations Population Division], 2016. http://www.internetlivestats.com/internet-users/india/

[39] PTI/The Economic Times; "Mobile users may constitute 80% of Internet users by 2017", The Economic Times, Bhopal, Feb 20, 2016 http://economictimes.indiatimes.com/tech/internet/mobile-users-may-constitute-80-of-internet-users-by-2017/articleshow/51070141.cms

[40] The reference here is, to a state where one is dutiful, conscious, resolute and diligent in, and to the study of a topic (in this case privacy) http://www.thesaurus.com/browse/with+eyes+wide+open

[41] *"Cultural Transmission"* is the transmission of preferences, beliefs, and norms of behavior which is the result of social interactions across and within generations [20].

[42] *Ibid*


रजिस्ट्री सं० डी० एल०—(एन)04/0007/2003—16 REGISTERED NO. DL—(N)04/0007/2003—16

भारत का राजपत्र
The Gazette of India

Cognizance of offences. 47. (1) No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorised by it.

(2) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act.

PUBLISHED BY AUTHORITY

सं० 19] नई दिल्ली, शनिवार, मार्च 26, 2016/चैत्र 6, 1938 (शक)
No. 19] NEW DELHI, SATURDAY, MARCH 26, 2016/CHAITRA 6, 1938 (SAKA)

Fig. 2 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016. Chapter VII (Offences and Penalties), Section 47. Source: Government of India

Universal Declaration of Human Rights,[43] International Covenant on Civil and Political Rights (ICCPR),[44] and International Covenant on Economic, Social and Cultural Rights (ICESCR).[45]

In direct relationship to the aforementioned conventions to which India is a signatory, it will be worth noting, at least philosophically, that, the European Parliament has recognized that any understanding and any "assessment of a Western-type human rights model against an Asian background [will] by no means [be] an easy task, given the big differences in the cultures involved [21]." So, for those who would argue that the privacy protection frameworks to be conceived and instituted in India should (or need) not look or feel like anything similar to what the EU has in place, and that India's cultural differences might not permit such alignments,[46] one has to ask the following question regarding 'privacy as a human right' - for certain. That question being: what exactly did it mean for India - to accede to the International Conventions above, if the Country's founders and her subsequent leaders/administrators did not (or do not) believe in granting Indian Citizens, those human rights 'most fundamental to all' in the world irrespective of colour, creed, faith, sex, education, beliefs, culture and socio-economic standing etc.? Contrastingly however, and surrounding India are, other nations of the world like China, that are speeding on ahead, in terms of their adaptivity to technology, and improvements in societal laws and practices to assist their standing in the world.[47]

6 Social corruption

In the opinion of many in the know, *the Aadhaar* scheme is the biggest violation of an individual's right to privacy that this world has witnessed, especially given the fact that nearly 1.4 billion of the World's population is involved.[48] What was once sold to the Indian taxpayer as an aid to curb corruption, inefficiency and waste of resources appropriated with taxpayer funds is now evidently just a 'big data gathering exercise,' which is allowing private companies primarily, to access and to use, in

[43] India was one of the original 48 nations of the world that voted to adopt the Universal Declaration of Human Rights (UDHR) in the General Assembly of the United Nations, on 10 December 1948

[44] Regarding the International Covenant on Civil and Political Rights (ICCPR) of 1966, India acceded to the Convention on 10 April 1979. India has not signed the ICCPR Optional Protocol I (1966) or ICCPR Optional Protocol II (1989)

[45] Regarding the International Covenant on Economic, Social and Cultural Rights (ICESCR) of 1966, India acceded to the Convention on 10 April 1979, but, India has not signed the ICESCR Optional Protocol (2008)

[46] Subhajit Basu, *supra* ref. [15]

[47] The Standing Committee of China's National People's Congress, passed the "Decision on Strengthening Network Information Protection" (the "Decision"), on December 28, 2012. [In brief, "the decision" asserts certain basic principles related to personal privacy and information security. The Decision asserts for example that 1) any personal electronic information collection by entities must be preceded by published (known) policies regarding all data practices by such entities, that 2) parties, whose information is being collected must be informed of the purpose of collection, method and the scope of data collection, and that 3) the collectors of personal information must obtain prior consent of those individuals whose information they intend to collect. In addition, the Chinese Ministry of Industry and Information Technology's (MIIT) *"Guidelines for Personal Information Protection Within Information System for Public and Commercial Services (2013 Guidelines), effective in 2013, is another noteworthy rule-making effort. It aims to create a systematic framework of personal data protection in computer and information networks. 2013 Guidelines draws a line between "personal sensitive information" and "personal general information", the former referring to information that "would have an adverse impact on the subject of personal information if disclosed or altered" including one's ID card number (similar to social security number in the US), biometric information,* etc. *It sets forth eight "basic principles", including personal consent, public notification, and minimum sufficiency, that govern the whole process of personal data collection and processing."* It has been additionally noted that, even in the absence of stringent information management related enforcement practices in China today, that, in the overall, *"the 2013 Guidelines has a "very careful structure and considerable detail", suggesting that "China is moving away from having a patchwork of largely unrelated sectoral data privacy laws (somewhat like the US) toward a more coherent structure."*"– Han [22]

[48] Sabreen Ahmed & Shubhankit Singh Sengar; "Right to Privacy- Is UIDAI A violation of An Individual's 'Fundamental Right'?," World Journal on Juristic Polity, November 2016. http://jurip.org/wp-content/uploads/2016/12/Sabreen-Ahmed.pdf And "Issues for Consideration: Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016", PRS Legislative Research - Institute for Policy Research Studies, New Delhi, India, 9 March 2016 – When law enforcement and intelligence agencies use the Aadhaar number to cross-reference various datasets consisting of telephone records, air travel records etc. to recognise patterns of behaviour of people, there are no protections for those innocent citizens who could be misidentified as potential threats against the State. Also, "the Bill [now law] empowers the UID authority to specify demographic information that may be collected ..... This power now permits the authority to collect additional personal information, without prior approval from Parliament." Lastly, "the Bill [now law] does not prevent the UID authority from requiring the collection of biometric information such as DNA." And Speech on Aadhaar by the author in House of Representatives (Lok Sabha), Parliament House, New Delhi, Republic of India, 11 March 2016 - https://www.youtube.com/watch?v=-2wSHjGCV5U

any manner they wish, the highly sensitive information of Indian citizens - within Indian government systems.[49] The harms that such a violation of personal privacy would entail are only just surfacing in the past few months. Various news and views published in the recent past throw immense light on the many irregularities associated with the biometric data collection program undertaken in India. It may sound far-fetched now, but, so much of the data collected, could possibly lead to the realization of outcomes and themes, now vividly portrayed in the highly popular 'Black Mirror' TV series.[50] It is socially and morally troubling to meditate upon, how such situations could play-out in a milieu of mostly illiterate populace.

7 System & Security Failures

Relating to the proposal to install a unique, biometric ID system in the United Kingdom, a number of researchers located at the London School of Economics and Political Science performed a variety of analyses [24]. The researchers discovered that it would be an impossible task to guarantee the safety and security of such a vast and sensitive informational database, likely to be accessed millions of times a day and perhaps facilitating an equal number of transactions all over the UK. The research report cited the Prime Minister's Official Spokesman at No. 10 Downing Street - to have said:

> "The national register of information would be protected and people had that assurance. – Morning press briefing (25 May 2005)[51]

To this view by the PM's Spokesman, the EPG/LSE researchers rebutted the Prime Minister's perspective in the following way:

> "In guaranteeing that the national identity database will be secure, the government is ignoring precedent. No database's security can be guaranteed, particularly one that contains this amount of information, which will likely be accessed millions of times every day, with data changed on thousands of individuals every day, and particularly when this information is so valuable."[52]

In 2010, the UK government passed legislation to repeal the project.

With respect to *the Aadhaar* program in India, there are reports almost every day about data leaks originating from Government websites where sensitive biometric information of citizens, including their caste, religion, bank account details, address, next of kin and more, is being made publicly available for anyone to access through a simple Google search. On 1 May 2017, the not-for-profit Centre for Internet & Society revealed in a report[53] how four Government resources were the originators of the biggest public leaks of the sensitive information of 135 million people; which amounts to ~10% of India's total population.

The government and Unique Identification Authority of India (UIDAI), continue to *turn a blind eye* towards this massive leak, and have tried to set it aside simply as an aberration. They refuse to acknowledge the immense security risk the government itself is placing its citizens in, and continue to push aggressively for the wider implementation of *the Aadhaar* program.[54] In a recently published article, one of the chief proponents of *the Aadhaar* program, and a former CEO of an Indian corporate giant, also widely hailed as the *'Father of The Aadhaar',* has stated that smart mobile phones leave the user bereft of any privacy anyway, so what further wrong could *Aadhaar* commit.[55]

The government has been making *Aadhaar* mandatory for availing numerous schemes like State rationed items, State guaranteed employment, old age pension, crop insurance, disability welfare, meals for school children and even compensation for victims of the Bhopal Gas Tragedy.[56] The government has condoned such actions and its continuation, despite the Supreme Court's provisional order that explicitly said, *Aadhaar* could not

[49] Shashank Bengali; "India is building a biometric database for 1.3 billion people — and enrollment is mandatory," The L.A. Times, 11 May 2017 http://www.latimes.com/world/la-fg-india-database-2017-story.html and Kiran Jonalagadda; "A Rant on Aadhaar," 6 December 2016 - https://medium.com/@jackerhack/a-rant-on-aadhaar-6213e002f064

[50] *Black Mirror* is a dystopian anthology miniseries (UK/US), that in many ways, showcase technological encroachments on selfhood, made potently deviant by the perversion of systems of governance (government), and the debauching of personal morality. –Margaret Lyons; "Black Mirror's Frightening Excellence," Vulture, December 4, 2014 http://www.vulture.com/2014/12/black-mirrors-frightening-excellence.html and, "… to revere our digital gizmos is to become their pathetic slave." – Monahan [23]

[51] *Ibid*

[52] *Ibid*

[53] Amber Sinha and Srinivas Kodali; "Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information" (CIS Report on Aadhaar leaks), The Centre for Internet and Society, New Delhi, India, 16 May 2017 - http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/at_download/file

[54] *Ibid*

[55] Anirban Sen; "The biggest privacy risk is your smartphone: Nandan Nilekani," The Mint, 5 May 2017 http://www.livemint.com/Companies/uqfbdvlddwsaqDnFMTaqmM/The-biggest-privacy-risk-is-your-smartphone-Nandan-Nilekani.html

[56] Indo-Asian News Service "Aadhaar Card Becomes Mandatory For Bhopal Gas Victims," NDTV 28 Apr 2017 - http://www.ndtv.com/india-news/aadhaar-card-becomes-mandatory-for-bhopal-gas-victims-1686828

be made mandatory for any welfare schemes.[57] Ground reports indicate that there are massive amounts of errors arising when citizens go to avail their rightful welfare. Their fingerprints are not matching, disabled persons are being refused acknowledgement (and even enrollment), old people with ageing eyes are not able to get authenticated through iris scans, and all of them *en masse,* are being refused services.[58] After bulk of the citizens' data have been collected, *Aadhaar* is now becoming an exclusionary rather than being an enabler and inclusive tool, as it was originally proposed.[59]

For instance, beneficiaries of India's Mahatma Gandhi National Rural Employment Guarantee scheme have stated that they were compelled to sign a form expressing their consent to *Aadhaar* enrollment, as a condition to drawing benefit *(*quid pro quo*)*, by the administrative staff. In a rush to meet targets, beneficiaries were enrolled under *Aadhaar* cursorily. The ensuing turmoil was such that it led to many errors in linking *Aadhaar* numbers to the personal bank account numbers of the workers, thereby causing immense problems during payment of wages.[60]

To add insult to injury, in the span of 1 week - during late February and early March of this year - the government of India made the use of *the Aadhaar* obligatory to access 11 more government programs, such as mid-day meals for school children, scholarships for disabled citizens and job training help for women rescued from sexual trafficking.[61] Imagine the horror that a woman would have to bear – after having had to sum-up all courage to overcome psychological and sociological horrors, and other physical harms endured while being sexually trafficked – to needing to re-live those horrors because her most critical and personal information was compromised by an illegal, unethical and untrustworthy surveillance system run by her own government.

8 *The Aadhaar* and a contemporary inspection of its social implications: Surveillance and segregation

In April of 2017, Justices AK Sikri and Ashok Bhushan asked the Attorney General (AG) of India Mukul Rohatgi, "How can you make *the Aadhaar* card mandatory when we have passed an order to make it optional?"[62] Rohatgi citing fraudulent use of Permanent Account Number (PAN) Cards (issued by the Income Tax Department) and the siphoning of State funds to shell companies, and without offering any direct evidence to that affect, said, to prevent such type of fraud: "...the only option is to make *the Aadhaar* card mandatory."

The question that this parliamentarian has had, in relation to that event, and the courtroom question posed by the Supreme Court Justices, is the following. How is it possible that the Attorney General of India can demand the implementation of a practice that is largely unconstitutional, while choosing to contravene specifically the Supreme Court's earlier decision to utilize *the Aadhaar* program in only a voluntary capacity? How could the AG, in a Republic, and without taking the fundamental steps to ensure 'due-process of law,' unilaterally determine that his decision should assert ultimate validity for 1.4 billion people and that it was to carry legal sufficiency to make a corrosive program such as *the Aadhaar*, mandatory in Indian society?

Moreover, and importantly, in asking the court to make something that is unconstitutional - mandatory, nowhere was it clearly qualified how *the Aadhaar* program, which then had 440,000 fake students in just 3 Indian States officially enrolled [25], was going to be an adequate security barrier for all the fraud that AG Rohatgi was claiming to exist, and that which was supposedly funneling state-funds to shell companies. How could such an intrinsically flawed and mis-directed program, one that is neither safe nor secure, ensure to be that line of defense and purportedly be able to halt the flow of fraudulent funds into thieving hands? This question cannot be answered, for there is no moral and truthful answer. All in all, the level of technical, legal, social and political incompetence that has reigned around this issue remains too high-a-heap, to adequately sample here, and within the scope of this writing.

By making *the Aadhaar* mandatory, and in seeking a wider deployment for this savagery and repression of the digital age, the government of India is pushing for and toward ensuring the collection of even more data. At the same time, the government will be ignoring consequential actions that violate privacy each day, and for all times to

[57] Supreme Court of India - Writ Petition (C) No 494 OF 2012, Justice K.S. Puttaswamy (Retd.) & ANR. v. Union of India & ORS., New Delhi, India, 15 October 2015 (Supreme Court Order on mandatory nature of Aadhaar) https://drive.google.com/file/d/0B5mBxP7jq8_IS3R1RVJsOTZrRDg/view

[58] "Aadhar trouble: How a woman's wages under MGNREGA were transferred to someone else's account," Scroll,in, 9 April 2017 - https://scroll.in/newsrepublic/833487?s=cm

[59] Anumeha Yadav; "Rajasthan presses on with Aadhaar after fingerprint readers fail: We'll buy iris scanners," Scroll.in 10 April 2016 - https://scroll.in/article/806243/rajasthan-presses-on-with-aadhaar-after-fingerprint-readers-fail-well-buy-iris-scanners

[60] Anumeha Yadav; "Chhattisgarh's way of dealing with Aadhaar: When fingerprints fail, take photos," Scroll.in (21 December 2016 - https://scroll.in/article/822764/chhattisgarhs-way-of-dealing-with-aadhaar-when-fingerprints-fail-take-photos

[61] Mridula Chari, Anumeha Yadav & Shreya Roy Chowdhury; "Not just mid-day meals: Aadhaar made mandatory for 11 more schemes, violating Supreme Court ruling," Scroll.In [Identity Project], 05 March 2017

[62] ANI; "Supreme Court reserves its order on Aadhaar-PAN linkage" The Deccan Herald, 4 May 2017 http://www.deccanchronicle.com/nation/current-affairs/040517/supreme-court-reserves-its-order-on-aadhaar-pan-linkage.html

come, all throughout the various Indian government departments.[63]

The push is on, to make *the Aadhaar*, the 'base ID' scheme to which all government services and personal details of every citizen are getting connected. One *Aadhaar* number connected to all bank accounts, tax details, driving licenses, government benefits and every other aspect of a person's life. It is fast becoming the ultimate tool for effective government surveillance. And quite probably, in an uncertain future, this device will be a very dependable tool for ethnic cleansing. Such a thought could have only been considered as preposterous, if relatable and observable facts had not provided evidence to the contrary. Disability activists have long complained that *the Aadhaar* program is an exclusionary system,[64] which neglects the needs of the disabled, who were declined, repeatedly, to be enrolled in *the Aadhaar*. Fact remains that the disabled and elderly[65] continue to experience significant difficulty in enrollment, and many have routinely and continually been experiencing denials in essential services.[66]

By connecting every aspect of a citizen's life to this one number, the centralized bureaucratic system of power in this case can easily and efficiently keep track of the activities of every person resident in India. By such actions, this program has the potential of causing catastrophic individual and communal harms, if citizens' sensitive information should fall into the wrong hands.

At this time, it is important to remember that *the Aadhaar* Act's provisions could require the use of DNA as 'biometric information' in the future. Given the many advances today, in the field of genetics, a DNA enabled *Aadhaar* card will open up possibilities of segregating, isolating or excluding citizens based on their race & ethnicity, under some despotic future regime. Only the limits of one's imagination could perhaps limit how such tools could be redirected from original designs and be used by some in India to pursue wicked outcomes, given communal frictions and ethnic divisions spanning centuries.[67] The preceding statement needs to be qualified. It is presumed that all Indians are of the same stock. However, recent studies[68] have shown that Indians exhibit different ethnic and genetic variations. Therefore, the possibility of some future ruler turning against one particular ethnic group in India would not be all together implausible.

These auguries might sound dystopian at this point of time, but all the tools to make these prognostications a reality already exist. The only factor required to push for this fatalistic future to be made a part of our present, is the rise of a despotic ruler, who has a specific strain of hatred towards a class/creed/religion or race of people. Given the racial and ethnic divisions in India, which have taken shape over centuries, and the political climate across the world today, the possibility of such a person coming into command and to be possessing an array of phobias, strong aversions and the power to freely act on the hate-filled thoughts, cannot be ruled out entirely.

History vividly tells us of the atrocities that Adolf Hitler was able to commit against Jews, with a simple cloth armband, and a paper register. The possibilities to use *the Aadhaar* program as a surgically precise tool for mass surveillance is obvious, especially when one cares to notice how it is designed, and how it is now being foisted upon a largely unaware population as a 'must have'. Another example where a National ID was used to unleash genocide, where an estimated 800,000 human beings were massacred in a period of 100 day was in the Republic of Rwanda.[69] There, National ID cards, which identified Rwandans by tribal affiliations, were used effectively to engineer the mass murder of populations.[70]

Tribals (known as *Adivasis*) in India are currently facing a huge problem.[71] It is mostly amidst the tribal inhabited interior areas that valuable minerals deposits are found. The *Adivasis* occupying large tracts of land in the interior are being subjected to extreme inhuman atrocities, and are now being forcibly evicted from their lands and their homes by government agencies, often with the involvement of para-military forces sent to

[63] Government websites are leaking Aadhaar numbers. Who will take action against the government, Scroll.in, 25 April 2017 - https://scroll.in/article/835546/the-centres-casual-response-to-aadhaar-data-breaches-spells-trouble

[64] Chandreyee Ghose and Debraj Mitra; "Adhaar agony for disabled - Multiple rejections in one-track system," The Telegraph, Calcutta, 21 March 2017

[65] Christin Mathew Philip; "Aadhaar enrolment proves tough on elderly, disabled," The Times of India, 13 July 2013 http://timesofindia.indiatimes.com/city/chennai/Aadhaar-enrolment-proves-tough-on-elderly-disabled/articleshow/21048381.cms

[66] Can Technology Solve India's Biggest Problem?, The Wall Street Journal, 12 January 2017 https://www.wsj.com/video/can-technology-solve-india-biggest-problem/80D7413C-3EE3-49FA-A921-29DD1A1A3E1A.html

[67] Maria Thomas; "Hindu nationalists are trying to create designer babies that are fair, strong, and smart," QUARTZ, 9 May 2017 https://qz.com/979007/rss-hindu-nationalists-are-trying-to-create-designer-babies-that-are-fair-strong-and-smart/

[68] Mait Metspalu and Irene Gallego Romero et al.; "Shared and Unique Components of Human Population Structure and Genome-Wide Signals of Positive Selection in South Asia," The American Journal of Human Genetics, Volume 89, Issue 6, 9 December 2011 http://www.cell.com/AJHG/abstract/S0002-9297%2811%2900488-5 and 'Priya Moorjani, Kumarasamy Thangaraj et al.; "Genetic Evidence for Recent Population Mixture in India," The American Journal of Human Genetics, Volume 93, Issue 3, 5 September 2013 http://www.cell.com/AJHG/abstract/S0002-9297(13)00324-8

[69] Gregory H. Stanton; "The Rwandan Genocide: Why Early Warning Failed," Journal of African Conflicts and Peace Studies: Vol. 1, Issue: 2, September 2009

[70] James Fussell - Genocide Watch (PGI); "Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing," Seminar Series - Genocide Studies Program, Yale University, New Haven, CT, USA 15 November 2001

[71] Satbir Singh; "India: Mining, conflict and Adivasis," Minority Voices Newsroom, 29 June 2012 http://www.minorityvoices.org/news.php/fr/1163/india-mining-conflict-and-adivasis

enforce the government's unilateral decisions on eviction; all this in the sole interest of large corporations.[72] It is noteworthy that *the Aadhaar* is being meticulously and stringently implemented in *Adivasi* areas.

The Aadhaar card for a citizen can easily be sourced to be a 'one-stop-shop' to acquire all the information on any particular person, and to track them categorically. Whenever a citizen uses the authentication mechanism associated with her/his *Aadhaar* number, alerts will be dispatched to various entities regarding each of the activities, and of all her/his movements. Given the extent to which citizen activities will be mapped through *the Aadhaar* program and their participation in, either government programs and services, or other more public activities such as rail travel, land and property sale and purchase and banking services, if, and when, this tool is used for insidious purposes, the destructive societal implications of this program will be catastrophic. Creating and nurturing such an ever-growing instrument of *evil* design, with no safeguards, and other protective measures being unavailable to a citizen, and at a supremely high cost to the taxpayer, is not seemingly intended to serve any humane or social empowerment goal. The reader is specifically reminded that *the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016, Chapter VII (Offences and Penalties), Section 47* explicitly prohibits all citizens (See Fig. 2) from the ability to either launch a legal complaint, or a civil suit, for example, in relation to any aspect of the administration of *the Aadhaar* program or services, and, or, for any harms that may be suffered by an individual or party. Consequently, Indian citizens have no ability to protect themselves when harm occurs.

On 3 May 2017, in presenting arguments before the court related to *the Aadhaar* Program, the Chief Law Enforcement Officer, the Attorney General of India (AG) shocked the world when he declared before the highest court in the land that the Citizens of the nation – widely acknowledged to be the world's largest democracy, "do not have absolute rights over their own bodies," (See Fig. 3) in essence - declaring that the Government of India could lay claims to "one's self," on demand. The AG, however, did not elaborate then, just how, when, or under what specificities, such demands could be presented before a citizen by the State. However, in this author's view, the AG has struck a match, which is sufficient to spark a Constitutional Crisis.


LET TRUTH PREVAIL

THE TIMES OF INDIA

Citizens don't have absolute right over their bodies: Govt

Can't Refuse To Give Digital Samples For Aadhaar: AG

Aadhaar must for birth cert in Ggn

Newborns in Gurgaon are being enrolled for Aadhaar right after birth. Soon after birth, the infant's photo, name, address and parents' details with the enrolment or Aadhaar number of either parent is

UIDAI dismisses data leak report

UIDAI rejected a report about the leak of Aadhaar numbers and linked accounts, saying on Tuesday that there is no breach in its database and the issues flagged are not related to it. However, an

lying for PAN number from July 1 this year. The Centre also said after the passage of the Aadhaar Act, it has become mandatory for citizens to get the unique identity number. Rohatgi said that people could not claim to have the right to be forgotten by refusing to get an identification proof like Aadhaar. "Even if

Fig. 3 Front Page Story - Times of India 3 May 2017. Attorney General of India Notified The Nation's Highest Court That Indian Citizens Do Not Have The Right To Self-Determination. Source: Times of India

Apart from the fact that the Republic of India has a democratic system of government, the nation is also a signatory not only to the Universal Declaration of Human Rights but to a whole plethora of international agreements on very many Rights for the citizens. On all fronts then, this primarily means, both at the constitutional level and in terms of India's accession to the aforementioned international covenants, that the Indian government, various Indian governmental instruments and its agents are responsible to extend to every Indian Citizen, in every respect, all importance, all considerations and all deliberations concerning unenumerated and enumerated rights, bequeathed under the Constitution of the Republic, and that the same entities mentioned above will additionally harmonize, and complementarily extend, any and all other rights, acknowledged as being fundamentally universal human rights. In all these respects, the *'right to self-determination* [26, 27]*,'* is a universally fundamental human right for peoples, and for all Indians, therefore.

That which the AG has in effect said, and as Chief Law Enforcement Officer of the nation is, that he has personally determined that Indian Citizens to not be worthy of being afforded the *right to self-determination.*[73] Perhaps, it is high time that the Indian Parliament debate the issue of having the AG's outlook reoriented, on-account of the simple fact that he is neither schooled properly on rights that are constitutionally conferred upon every Indian Citizen, nor is he intimate with the details of those important international human rights conventions to which his country has acceded. Such is the nature of complex conundrums that India has to face daily in terms of privacy.

New rules related to *the Aadhaar* program seem to appear daily, and seem to do so without any Parliamentary advise, or

[72] Tania Murray Li; "Indigeneity, Capitalism, and the Management of Dispossession," Current Anthropology, Volume 51, No. 3, June 2010 and Felix Padel; "Investment-Induced Displacement and the Ecological Basis of India's Economy," In: "Globalisation and the Challenges of Development in Contemporary India" (Dynamics of Asian Development), Sita Venkateswar & Sekhar Bandyopadhyay [Eds.], Springer, 15 March 2016 https://link.springer.com/chapter/10.1007/978-981-10-0454-4_8

[73] *Ibid*

consent.[74] In light of such occurrences, it is impossible to comprehend how it is possible for a nation like India with broad societal differences, to be able to afford value to procedures and practices related to privacy, when the Attorney General of the country, who has the legal responsibility to protect and defend all Indians, has willfully made such deplorable, intellectually underfed and morally shriveled statements.

Although the Indian Supreme Court has been feeble on all matters related to *the Aadhaar* program, especially on matters related to privacy, it remains the last bastion for hope and sanity to prevail in India. However, we must consider that the highest court in India is also a reflection of those in Indian society that have a careless outlook towards Privacy. At present, the court seems to demonstrate no clarity or conviction of its own related to the importance of privacy, and is seemingly capable of acquiescing to a push by a few - toward imposing a national ID card for all. The inherent tensions between the various pillars of this democratic republic – the legislature and the executive on one, and the judiciary on the other, have also come to play a role in the rulings by the Judiciary. This case of protect the 'Right to Privacy' of citizens is also being subject to the tumultuous, turbulent times that India is going through after 70 years of Independence from the British. We, as a society, are evolving. One hopes that the courts shall follow.

The awareness about the possible ways in which *the Aadhaar* can be misused is growing extremely slowly in India.[75] Unfortunately, most people have not - the slightest understanding of the implications of their personal privacy being violated, their bodies being tagged & surveilled. Meanwhile, it must be admitted, political discourse has completely died out on this subject as the bureaucracy and big business interests have, together, pushed *the Aadhaar* program with extreme vigor on all political fronts equally. *The Aadhaar* was born when the Indian National Congress (INC) was in government. The Bharatiya Janata Party (BJP), the primary opposition of that time and its leadership including Mr. Narendra Damodardas Modi, the Prime Minister today, had vehemently opposed it earlier. However, in the 2014 general elections, the tables were turned. The BJP won, defeating the INC, and has been in power since then. Still, *the Aadhaar* is being implemented, despite their initial opposition to it, and with increased vehemence now. Smaller regional political outfits seem not to even notice the existence of *the Aadhaar*. In this bleak background, one can only hope that good collective public sense prevails and this harmful *Aadhaar* program is scrapped.

[74] Mridula Chari, Anumeha Yadav & Shreya Roy Chowdhury, *supra* note 62

[75] Manish Singh; "India's database with biometric details of its billion citizens ignites privacy debate," Mashable, 14 Feb 2017 - http://mashable.com/2017/02/14/india-aadhaar-uidai-privacy-security-debate/#E9emBilGXOqr

9 Privacy state in India: A forward look beyond *The Aadhaar*

In an Harvard Business Review article called *"Values in Tension: Ethics Away from Home* [28]*,"* Tom Donaldson of the Wharton School of Business painted a tale of how, in the 1980, European tanneries and pharmaceutical companies shopped around the world, for cheap waste-dumping sites; countries where those companies could unload highly toxic wastes. Those companies found Nigeria to be a willing taker of the Poly-Chlorinated Biphenyls (PCBs) that the European companies wanted to unload. Donaldson describes Nigerian workers with no protection whatsoever, receiving highly toxic PCBs, and then depositing them next to Nigerian residential areas, where neither the workers, nor the residents were made aware of the locating of the PCBs in their neighborhood, or of the PCB's toxicity. By the presentation, Donaldson wanted to have the reader adequately contemplate the application of the requisite template for ethical business conduct, both domestically and internationally. Interestingly, the speed and rates of modern business data and other forms of information flows have curtailed such practices as Donaldson describes, but have not altogether eliminated them, as *the Aadhaar* demonstrates in India today.

However, strangely, Donaldson's story is useful to analyze what lies ahead for India in terms of privacy. At present, and in a certain way, India is similar to Nigeria in the case above; terribly unaware of the dangers associated with the loss of privacy, and dreadfully unfazed by the plethora of risks that loss of privacy poses to every single Indian citizen.

10 Privacy context specificity to India's economic future

It is this author's assessment that the reliability, robustness, stability, safety, and security as it is related to the shaping of India's privacy framework will decidedly shape the nation's economic future also. For Indian politicians, at a very personal level, the lack of understanding of technological contextualization needs, in terms of India's strategic development tracks, economic and political myopia, and a lack of tactical and strategic understanding of technology development cycles and their applicability to India - puts the country's leadership (their friendships with tech-titan CEOs aside), at a clear disadvantage.

Micro, Small and Medium Enterprises (MSMEs) constitute the present day backbone to the Indian economy. MSMEs now employ in excess of 110 million of workforce, and now account for - in excess of ~37% of India's GDP [29]. However, future growth in this sector can only come at the expense of training that is more multi-sector,

greater technology awareness and greater connectedness to the vital construct of privacy. Personal Privacy in the Digital Century is translatable synonymously to the safety and security of information technology assets and the critical information that it holds, anywhere. In this sense, Privacy and Informational Safety and Security are one - and the same.

Therefore, India's ability to offer vibrant Information Technology Enabled Services competitively, and in a changing word, is inextricably linked to the country's ability to recognize the critical value of privacy, and the established need for the security and safety of information, and information systems. In the here and now, the twenty-first century, and in the midst of the fourth industrial revolution, India must ensure to have in place, for her citizens, the most fundamental of human rights to which she had acceded in 1948, but has yet to deliver upon.[76] Directly to India's economic future, is the necessity for India to demonstrate to her trade partners that she is a developed, mature, and wise member among the community of World nations.

Importantly and structurally, in this regard, India must instrument privacy, information safety and security policies and practices. Also, India must connectedly establish those means and methods for oversight, enforcement, legal intervention, adjudication and the means to suitably recompense injured parties in those case where there are infractions, or when losses are sustained.

11 Privacy related contextualization example: India-EU economic relations

To materially contextualize, it should be understood that the EU is one of India's vital trading partners (14% of India's overall trade in 2015–16).[77] Even though the Broad-based Trade and Investment Agreement (BTIA) that was being negotiated between India and the EU has stalled, economics is the fundamental driver for a strategic alignment with the EU which kicked-off with the EU-India Strategic Partnership arrangement in 2004. Not only is the EU India's biggest trading partner, but, in the last 15 years, EU member countries have made more Foreign Direct Investment (FDI) into India, than the US and Japan combined,[78] and in spite that Mark Zuckerberg and Narendra Damodardas Modi are BFFs.[79]

Maintaining the logical thought connection as related to privacy, information technologies, and India's economic future, the following considerations must be made. India is the world's largest Offshore IT sourcing destination, accounting for 67% of the US$ 130 billion outsourcing market [30]. And, India has had over 25 years of experience in Business Process Offshoring (BPO), being the destination of choice for the outsourcing desires of Western companies overall.[80] In dealing with Indian firms for the better part of 25 years and more, Western companies did not choose India for its willingness to accept toxic waste. Rather, India had offered highly competitive services at attractive and lower cost points, match for timeliness, higher quality performance, and a general prospect for higher business profitability. The Indian BPO sector now employs over 3.7 million people, experienced record annual growth of 10%.[81] The IT Enabled Services (ITES) (BPM - Business Process Management and BPO-Business Process Offshoring) sector in India is estimated to expand at 10% (CAGR) to a whopping US$ 300 billion by 2020. The IT sector as a whole is expected to triple to US$ 350 billion by FY 2025. With respect to Europe directly, and in 2016 alone, India provided EU with its lion-share of IT services totaling US$30 billion.[82] However, BPO involving the handling of increasingly sensitive "Information" items such as telemedicine data from the US and the EU have been changing over time, as regulations involving Information exchange and management in other countries have been becoming stricter. India has been standing still in this area of sensitive information handling, as fundamentally, constructs relating to privacy have been alien to Indian society, even with a robust IT/ITES sector within the country.

Consequently, BPO growth is expected to be undermined dramatically, owing to immense changes happening in the world of Privacy, where again, India has virtually stood still. India does not have a meaningful national Privacy Law, nor does it have a central government Data Protection and Privacy Officer. At present, individual Indian States also do not have necessary privacy protection mechanisms that are either suitable or conducive to attracting business prospects from those foreign countries who will intend to originate data - that may later be handled in India. In the absence of reliable, durable, safe and secure privacy laws and accompanying durable structures to manage and maintain information, other outsourcing destination points (countries) like the Philippines may appear more attractive for overseas businesses.

Although an American perspective, Barbara George and Deborah Gaut frame the threat that India faces in this respect well, and their characterization is widely applicable. They say:

[76] India was one of the original 48 nations of the world that voted to adopt the Universal Declaration of Human Rights (UDHR) in the General Assembly of the United Nations, on 10 December 1948

[77] Source: Director General for Trade, European Commission - Trade Picture (India), 7 April 2017

[78] Directorate-General for External Policies - Policy Department; "Evaluation of the EU-India Strategic Partnership and the potential for its revitalisation" [report generated at the request of the European Parliament's Committee on Foreign Affairs, by Gulshan SACHDEVA - JNU], Brussels, Belgium, June 2015

[79] BBC; "Modi hails social media power at Facebook HQ," 28 September 2015 http://www.bbc.com/news/world-asia-india-34376778

[80] Source: NASSCOM – India IT BPM Overview, 2015

[81] *Ibid*

[82] *Ibid*

> India's cultural history is a significant factor for American outsourcers to consider in pressing for either data privacy legislation in India or protective contractual provisions with Indian companies. Indian cultural history may affect Indian companies' interpretation of the concept of privacy, which will affect the degree of importance that India as the host country is willing to place on the protection of privacy. A pertinent statement appears in The European Union's Assessment of Adequacy, a report addressing the effect of differing political and cultural values on interpretations of standards of "adequacy" of data privacy protection measures to meet the E.U. standards:
> A final difficulty is that of cultural and institutional non-equivalence. Judgments about adequate protection must remain sensitive to important cultural differences. Despite the growing convergence of international data protection policy, 'privacy' still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone.... [31]

India has to be an attractive business destination for information technology companies in the digital century. However, to become that attractive business destination above all other choices in the digital century, it will require those in Indian government, industry and civil leadership to prioritize matriculating oneself into "night-school," with the intention to expeditedly acquiring their E-MBAs in Privacy, prior to the new law known as the General Data Protection Regulation (GDPR)[83] going into effect within the EU member States.

The Data Protection Directive of 1995[84] will soon be replaced with a rigorous and more codified privacy practice framework of the GDPR. That GDPR will undoubtedly be the de facto framework in force beyond data protection, for privacy, with which the Indian IT sector businesses will have to negotiate; and they are likely to negotiate badly, as Indian IT firms have historically found their ability to comply with the less rigid Data Protection Directive of 1995 in the EU (presently in force), most difficult.

If Indian firms are not prepared to comply with the GDPR's overall dictates, it is as Nasscom's former President, R Chandrasekhar had announced, that, "...security in Europe has the potential of going into directions which will not be conducive for (those) countries as well as our (IT) industry. They will get hurt and we will also get hurt." Lastly, a Nasscom-DSCI (Data Security Council of India) poll has revealed that there exists the very real possibility of "a significant opportunity loss for the IT-BPO industry on the account of data transfer related issues as clients hesitate to offshore work to India because of stringent data protection requirements in the EU [32]."

The idea of "Data Protection" encapsulates the concepts of privacy, and the safety and security of all information that IT systems house. Everything is inter-connected; and nothing can be disconnectedly considered, and singularly; such as the subject of safety apart from security, or privacy apart from security. At present, the EU's Data Protection Directive permits the transference of data originating from the EU to third parties – that is to say, countries beyond the EU, and the EEA, only if such a third party State has been determined by the EU as being "Data-Secure." Looked at - in another way, the EU Data Protection Directive mandates member States to forbid the 'transfer' of personal data to a non-EU member State, unless the State has demonstrably met all data protection criteria, having in place, "adequate" data and privacy protection methods, means, structures and systems.

India is not a "Data-Secure" State in the eyes of the EU.[85] However, for some time now, India has lobbied the EU for a "Data-Secure" State status declaration.[86] Naturally, the EU and, or other states cannot be expected to *"rubber-stamp"* such declarations, when the awareness of privacy and data protection constructs by the Indian workforce is generally weak, and is usually coupled to the existence of weak institutional policies, practices and frameworks related to information safety and security practices. The one widely available and discussed case of the theft of US$ 350,000 from 4 New York based clients of Citibank, by their call-center operators in Pune, India, operated by Mphasis (formerly MsourcE) has become the bane of Indian BPO firms.[87]

However, from a Safety and Security point of view, this case demonstrates some interesting things, if one investigates further, that are the following. The operating Call-Center had received a BS 7799 (UK) security certification, which meant that the Center had demonstrated meeting the desired best

[83] "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA," The European Parliament, Brussels, 27 April 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

[84] Directive 95/46/EC of the European Parliament and of The Council, "On The Protection of Individuals With Regard To The Processing of Personal Data and on The free Movement of Such Data," The European Parliament and The Council of The European Union, Luxembourg, 24 October 1995 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[85] "There is no adequacy agreement for India… [33]"

[86] "Data secure status for India is vital: Sharma on FTA with EU Sharma reiterated that Mode IV in services and data secure status are very important for India," Business Standard/Press Trust of India, September 3, 2013 http://www.business-standard.com/article/economy-policy/data-secure-status-for-india-is-vital-sharma-on-fta-with-eu-113090300889_1.html

[87] "BPO Staffers Hack Bank A/Cs, Steal Rs 1.5 CR", The Times of India, 6 April 2005 http://timesofindia.indiatimes.com/city/pune/BPO-staffers-hack-bank-A/Cs-steal-Rs-1-5-cr/articleshow/1070986.cms

practice methods for protecting information – meeting 'information confidentiality,' 'information integrity' and 'information availability' criteria. It also meant that the Center had demonstrated 'BS 7799 - Part 1' proficiency in the established standards of practices relating to 'information security,' and 'BS 7799 - Part 2' proficiency in practice specification for 'information security management systems.' What is more, the Center operated by Mphasis, by the company's own pronouncement, had undergone *"a comprehensive information security audit by the Standardization, Testing & Quality Certification (STQC) Directorate*[88] *covering Information Risk Management, Network Security, Physical Security, Personnel Security and Business Continuity Planning."*[89] Also that, MsourcE had especially "worked with"[90] the global accountancy and consulting firm of Ernst and Young to gain the certification. Additionally, the Center also received a CMM Level 5 quality certification.[91]

If after being certified in the aforementioned way, by recognized global standards, and by recognized global entities, it is possible for a facility with such certifications to sustain a breach, then, there is a valid cause for concern by entities like the EU. Just as everyone was beginning to breathe a sigh of relief, in less than a year, it happened again, when a HSBC Bank Data Processing Center employee accessed and used the "personal, security and debit card information" to pick-pocket 20 of the bank's U.K. - based customers to the tune of US$420,000.[92] Adjacently, an Indian forensic consultancy reported that the lack of institutional whistleblower policies/protections, fraud response plans and the lack of proper levels of ethics training of employees, were at least partially to blame for such security breaches [34].

When the EU-GDPR law does go into effect in 2018, it will likely become the de facto Data Protection and Privacy framework for the world, as all nations who will intend to, and currently do business with the EU member States, will have to comply with the GDPR in relation to all manners of conducting normal business. The widespread change effect that the GDPR will impose, and extract worldwide, will not go unnoticed in India.

In the meantime, in one hand, India has a Draft Privacy Bill[93] in various forms; and the last leaked version of it was the 2014 edition.[94] The Parliament has not seen any version of this Bill. In the other hand, is that law, which India would like to claim is her equivalent of a Privacy & Data Protection Law, one that would provide adequate protection related coverage for Data Protection and Privacy Protection – the one called the Information Technology Act of 2000, as amended in 2008.[95] There are only just a few major problems with these lines of arguments that IT sector representatives have managed to place forward. In a Confidential academic report to the European Commission, titled: "First Analysis of the personal data protection Law in India: Final report to the European Commission," the authors state:

> Although the Information Technology Act, 2000 is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30th January, 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its twenty-ninth session, it is often quoted in India as an Act containing provisions pertaining to data protection." "…In general, the IT Act is more an Act related to e-commerce and cyber crime than a data protection Act [35].

Furthermore, Graham Greenleaf as the party who performed a data and privacy protection "adequacy" assessment for the EU, and in accordance with the Data Protection Directive, Article 25, recommended that India's Data and Privacy Protection frameworks would not adequately be protective of that data transferred from the EU to India. Greenleaf, as part of his later assessment of IT Act of 2000, as amended in 2008, had the following to say. Greenleaf said,

> …the most important legislative protections are as yet, not functioning. In particular, the key data protection provisions of the 2008 amendments to the Information Technology Act 2000 are not yet effective, and the consumer protections in the credit reporting legislation appear to be ignored by regulators and credit bureaux alike [36].

Finally, it is this author's read that while the government has attempted to convey to the outside world through the

[88] Standardization, Testing & Quality Certification (STQC) Directorate of the Ministry of Electronics and Information Technology (MeitY), Government of India, New Delhi, India. http://meity.gov.in/content/stqc

[89] "MsourcE Customer Contact Center recommended for BS 7799–2: 2002 rating: International certification provides highest possible security to customers." MsourcE Press Release, 14 May 2003 http://www.mphasis.com/downloads/news/BS7799certification.pdf

[90] *Ibid*

[91] "The Five levels of CMM", CIO (IDG News Service), 1 March 1 2004 http://www.cio.com/article/2439787/enterprise-software/the-five-levels-of-cmm.html And [simple information source: Explaining "Capability Maturity Model (CMM)"
Management Library - Vector Study Group http://www.vectorstudy.com/theories/capability-maturity-model

[92] "Indian police arrest employee at HSBC outsourcing center for cheating U.K. customers," The Age (Australia) AP, 28 June 2006 http://www.theage.com.au/news/Technology/Indian-police-arrest-employee-at-HSBC-outsourcing-center-forcheating-UK-customers/2006/06/28/1151174255132.html

[93] Drafted by the Department of Personnel and Training, Government of India.

[94] Elonnai Hickok; "Leaked Privacy Bill: 2014 vs. 2011, "The Centre for Internet & Society", Delhi, India, 31 March, 2014

[95] Data Security Council of India/NASSCOM; "EU Adequacy Assessment of India" [Whitepaper], New Delhi, India, 7 January 2012

existence of "Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011", India has met key data and privacy protection "adequacies", the government will only be fooling itself. Despite the existence of Information Technology (Reasonable security practice and procedures and sensitive personal data or information) Rules, 2011, under s87(2)(ob) of the IT Act, and under section 43A', Graham Greenleaf's own words describe the situation best, that, *"India does not have a comprehensive data protection law covering any sector* [37]*."* Instead of clearly and constructively putting-together - a national Privacy & Data Protection Bill responsibly, that not only will adequately cover today's working needs, but will also allow for the necessary legislative flexibility and the socio-economic growth anticipated, and be capable of accommodating for constitutional protections for Citizens, India has chosen to implement the most difficult legislative choices. The government of India has decided to cobble-together, legislative elements that add complexity all the way around, while also blurring jurisdictional and adjudicational abilities.[96]

Lastly, with respect to the Draft Privacy Bill of 2011,[97] it is acknowledged that the legislation's "exclusion of the Indian government [activities] from the scope of the Bill [represents] a very severe weakness, particularly because there are so many privacy-invasive public sector projects going forward in India at present, including the national ID number, and NATGRID ... Some of this surveillance legislation also empowers private organisations to act as agents of the government in collecting data, probably outside this Bill."[98] In an assessment of the Bill's fundamentals as circulated, and unseen as yet by the Indian Parliament, it remains uncertain the implementation of Rules by Bill can deliver data protection in reality, or, if it will be "just an unenforceable illusion."[99]

We are essentially riders of bicycles with training wheels in thoroughfares which high-performance vehicles make their home. The mere fact that none have been hit or killed while in motion says nothing about *the muddle and strangeness this reality represents,* and is but a simple golden act of providence. Graham Greenleaf wrote in a later paper, criticizing the orientation and the functions of the as yet uncirculated and unintroduced Bill in Parliament; Indian Privacy Bill. It seems the Privacy Bill, and the protections it would afford the Private Sector in India would not apply to those in the Public Sector. It so appears that the World's largest democracy is intent on creating a national legal framework that proposes the erection of a "double standard" statute. Greenleaf qualified it best saying, *"[a] bizarre aspect of the Bill, for a country seeking an EU adequacy finding, is that it limits its protection to Indian businesses… India is therefore one of the few countries to have enacted data privacy laws for its private sector, but not for its public sector. That may not prove to be tenable in the longer run."*[100] If all this were not enough, like icing on a cake, the Indians are left to negotiate and to navigate an unconstitutional government sponsored surveillance and tracking mechanism called *the Aadhaar.*

12 Conclusion

At the present, the Republic of India does not have in force a comprehensive, clear, and robust Privacy law. Article 21 of the Indian Constitution has asserted the need to assure "protection of life and personal liberty." But, as in the case of the United States, India does not explicitly guarantee a Citizen's right to privacy. However, *Govind* vs *State Of Madhya Pradesh & Anr. (1975)*[101] and *Unni Krishnan, J.P. And Ors.* Etc. vs *State Of Andhra Pradesh And Ors. (1993)*[102] have recognized one's enumerated right to personal privacy.

In Govind vs State Of Madhya Pradesh & Anr., it was clearly asserted, for instance, that while one's right to privacy 'at the time' was not determinable by the court as being absolute, the court had ruled that restricting one's privacy, and in any way had to be upon *"the basis of compelling public interest",*[103] and that any infringement upon privacy, *"must satisfy the compelling State interest test."*[104]

[96] Greenleaf give us an example of complexities and the blurring of jurisdictional and adjudicational abilities when he states the following: "[g]iven that s43A does not purport to regulate anything other than 'negligen[ce] in implementing and maintaining reasonable security practices and procedures', it is difficult to see any legislative mandate for the Rules to impose any obligations other than those which can be described as 'reasonable security practices and procedures'. This brings into question how … Rules dealing with privacy policies, a variety of data protection principles, and disclosure of data …. can be enforced…." Graham Greenleaf, *Supra* (ref. [37])

[97] Privacy Bill of 2011, *supra* notes 94 & 95 [It is acknowledged that there is a 2014 edition that is in circulation. However, no version has appeared before the parliament for discussion, and/or deliberation]

[98] Graham Greenleaf, *supra* (ref. [37])

[99] *Ibid*

[100] Graham Greenleaf; "India's U-Turns on Data Privacy", Privacy Laws & Business International Report, Issues 110–114, UNSW Law Research Paper No. 2011–42, 2011 [Greenleaf has additionally noted: "India sought an 'adequacy assessment' from the EU in 2009/10 ... so it is clearly desirous of a favourable view from Europe, to ease compliance burdens in relation to outsourcing. The current state of India's privacy protections makes that a more complex question than it was a year ago."]

[101] Govinda v. State of U.P., [1975] 3 SCR 946 In this case reliance was placed on an US Supreme Court decision in the case of Griswold v. Connecticut, 381 US 479 at 510 (1965) https://indiankanoon.org/doc/1775396/

[102] Unni Krishnan, J.P. And Ors. Etc. vs State Of Andhra Pradesh And Ors., 4 February, 1993 [1993 AIR 2178, 1993 SCR (1) 594] https://indiankanoon.org/doc/1775396/

[103] Govinda v. State of U.P., *supra* note (102)

[104] *Ibid*

One of the most important points to note, and in relation to the aforementioned statement is, as follows. Being a member of the national legislature, this author can attest to the fact that no such *compelling State interest test* has ever been discussed, conceived, deliberated, consented to, or developed - with the cooperation and, or consent of the Parliament, in relation to *the Aadhaar* program. Additionally, and again as a member of the national legislature, this parliamentarian can further attest that, no *compelling state interest* in relation to the need to have *the Aadhaar* program deployed has ever been introduced, and, or formally brought forward for deliberation before the national legislature; either supported by results of any compelling national interest test, or separately by the widely acknowledged presence of any *compelling state interest*, which has been incontestably surfaced, and through incontrovertible means.

Also, it must be noted strongly that, in terms of deploying a program that would ultimately affect nearly 1.4 billion people, the many States in the Indian federalism have neither been adequately consulted, nor has the issue been adequately deliberated authoritatively. This is not a small process deviation in the least, or a democratic process breakdown at most, rather a demonstration of moral bankruptcy in the fabric of national governance.

Compliance with ethical standards

Conflict of interest The author declares no conflict of interest.

Funding There is no funding source for this article.

Ethical approval This article does not contain any data, or other information from studies or experimentation, with the involvement of human or animal subjects.

Informed consent Not Applicable

References

1. Anderson JF. The rhetorical impact of evil on public policy. Administration & Society. 2006;37(6):719–30.
2. Matsaganis MD, Gregory Payne J. Agenda setting in a culture of fear: the lasting effects of September 11 on American politics and journalism. Am Behav Sci. 2005;49(3):379–92.
3. Minnich E. The evil of banality: Arendt revisited. Arts Humanit High Educ. 2014;13(1–2):158–79.
4. Newsclick Production. Aadhaar: The Lies and The Realities…. Newsclick India, 17 Mar 2016 http://newsclick.in/india/aadhaar-lies-and-realities.
5. Alam M. Is caring for elders an act of altruism? Some evidence from a household survey in Delhi. [Expert Group Meeting - Intergenerational Solidarity: Strengthening Economic and Social Ties]. United Nations (UN Social Policy Division, Department of Economic and Social Affairs (DESA)), New York; 2007.
6. Ermisch J. An economic analysis of family. Princeton: Princeton University Press; 2003.
7. Cox D, Rank MR. Inter-vivo transfers and intergenerational exchange. Rev Econ Stat. 1992;74.
8. Rosell SA, et al. Changing maps: governing in a world of rapid change. Ottawa: Carleton University Press; 1995.
9. Chadha NK. Intergenerational relationships: an Indian perspective. [Department of Psychology], University of Delhi, Delhi. UN - Department of Economic & Social Affairs/Division of Social Policy & Development (DESA). 2012. http://www.un.org/esa/socdev/family/docs/egm12/CHADHA-PAPER.pdf.
10. Nayak DK, Behera RN. Changing household size in india: an interstate comparison. Trans Inst Indian Geographers. 2014;36(1). reflecting the last Census, taken in 2011.
11. Households by Type and Selected Characteristics: ACS 2011. American Community Survey. Washington, DC; U.S. Census Bureau, U.S. Dept. of Commerce; 2011.
12. Milberg SJ, et al. Values, personal information privacy, and regulatory approaches. Commun ACM 1995; 38(12).
13. Fjetland M. Global commerce and the privacy clash. J Inf Manag. 2002;36(1).
14. Bellman S, et al. International differences in Information privacy concerns: a global survey of consumers. Inf Soc. 2004;20(5).
15. Basu S. Policy-making, technology and privacy in India. Indian J Law Technol 2010;6.
16. Lalmalsawma D. India speaks 780 languages, 220 lost in last 50 years – survey. REUTERS September 7, 2013 http://blogs.reuters.com/india/2013/09/07/india-speaks-780-languages-220-lost-in-last-50-years-survey/.
17. Rama M, et al. Addressing Inequality in South Asia. Washington, DC; International Bank for Reconstruction and Development/The World Bank; 2015.
18. Lal V. "Manas" [Indian religion], School of Social Science, UCLA, Los Angeles. 2017. https://www.sscnet.ucla.edu/southasia/Religions/religions.html.
19. Matanhelia P. Mobile phone usage among youth in India: a case study. [PhD Dissertation]. University of Maryland, College Park; 2010.
20. Bisin A, Verdier T. Cultural transmission. Prepared for the New Palgrave Dictionary of Economics [Second Edition]. New York; New York University; 2005. http://www.econ.nyu.edu/user/bisina/Palgrave_culturaltransmission2.pdf.
21. de Hert P, Papakonstantinou V. The data protection regime in China: In-Depth Analysis. European Parliament [Directorate General for Internal Policies/Policy Department C - Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs], Brussels, Belgium; 2015.
22. Han D. The market value of who we are: the flow of personal data and its regulation in China. Media Commun 2017; 5(2). also, the MIIT 2013 Guide, at: http://www.pipa.gov.cn/manage/UploadFile/2015518133720563.pdf.
23. Monahan M. Black mirror: white christmas, review: 'Be careful what you wish for...'. The Daily Telegraph [UK], 16 Dec 2014. http://www.telegraph.co.uk/culture/tvandradio/tv-and-radio-reviews/11295878/black-mirror-christmas-special-review-the-nightmares-before-christmas.html.
24. Davies S, Whitley E. The identity project: an assessment of the UK Identity Cards Bill and its implications. EPG/LSE Report [Department of Information Systems, the London School of Economics and Political Science], London. 27 June 2005 http://eprints.lse.ac.uk/684/1/identityreport.pdf.
25. Worstall T. Aadhaar scheme uncovers 440,000 fake students in just three states. FORBES, 27 March 2017 https://www.forbes.com/sites/timworstall/2017/03/27/aadhaar-scheme-uncovers-440000-fake-students-in-just-three-states/#1b3dd3d95bc9.
26. What are Human Rights?. Office of the High Commissioner - Human Rights. Geneva: United Nations. 2017. http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx.

27. Thürer D, Burri T. Self-determination. Oxford Public International Law [Max Planck Encyclopedia of Public International Law (MPEPIL)] Dec 2008 http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e873.
28. Donaldson T. Values in tension: ethics away from home. Harvard Business Review, September–October 1996 https://hbr.org/1996/09/values-in-tension-ethics-away-from-home.
29. Mehta N. 'Only micro, small and medium businesses can provide maximum jobs, entrepreneurs and products for India'. [Academic Interest], The Times of India, 10 May 2017 http://blogs.timesofindia.indiatimes.com/academic-interest/only-micro-small-and-medium-businesses-can-provide-maximum-jobs-entrepreneurs-and-products-for-india/.
30. IBEF - India Brand Equity Foundation/TechSci Research, Ministry of Commerce & Industry, Government of India, New Delhi, India, April 2017 https://www.ibef.org/industry/information-technology-india.aspx.
31. George BC, Gaut DR. Offshore Outsourcing to India by U.S. and E.U. Companies Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing. U.C. Davis Bus. L.J. 6(2). 1 May 2006 http://blj.ucdavis.edu/archives/vol-6-no-2/offshore-outsourcing-to-india.html.
32. PTI. Data protection norms in EU may hurt Indian IT sector: Nasscom. Economic Times, 13 Jan 2014 http://economictimes.indiatimes.com/tech/ites/data-protection-norms-in-eu-may-hurt-indian-it-sector-nasscom/articleshow/28706032.cms.
33. Baker J. India pushes EU for data-secure status: Intellectual property is a key issue in trade talks. CIO (IDG News Service), 13 Sept 2012. https://www.cio.com.au/article/436364/india_pushes_eu_data-secure_status/#closeme.
34. Joshi M, Akkunoor P. Indian call centers woefully lacking in whistle-blowing policy and fraud response plan. Indiaforensic Consultancy services, Pune, India; 2006 http://www.indiaforensic.com/callcenter.pdf.
35. Fossoul V, de Terwangne C, et al. First Analysis of the personal data protection Law in India : final report to the European Commission (confidential). [Report To The European Commission: Directorate General - Justice, Freedom and Security], Faculty of Law, Law and Society Information Research Center, University of Namur, NAMUR, BE; 2005. http://www.crid.be/pdf/crid/5946.pdf.
36. Greenleaf G. Promises and illusions of data protection in Indian law. Int Data Priv Law. 2011; 1(1).
37. Greenleaf G. India's U-turns on data privacy. Priv Laws Bus Int Rep 2011;110–114. UNSW Law Research Paper No. 2011–42.