THE INDIAN IDENTITY PLATFORM "*AADHAAR*": IMPLICATIONS IN A DEVELOPING COUNTRY CONTEXT

Aradhya Sethia & Nimoy Kher
National Law School of India University (Bangalore)

INTRODUCTION

India's internet-driven 'Unique Identity' or *Aadhaar* Project, is the world's largest consolidated biometric database, containing the personally identifiable information (PII) of nearly 1 billion Indian residents. The *Aadhaar* platform, by linking biometric data with the distribution of essential public services, seeks to address major issues in identifying the beneficiaries of targeted government welfare schemes, which include under-registration, forged identities and resource leakage. These problems tend to perpetuate a vicious cycle of impoverishment and disenfranchisement, thereby hindering growth in some of the poorest regions on the globe. Indeed, *Aadhaar* has been projected as a 'technological panacea' to the structural socio-economic impediments, which have undermined the accessibility of basic goods and services in India. This paper, however, adopts a skeptical view towards *Aadhaar*.

This paper locates *Aadhaar* within the broader debate on networked governance and privacy theory. In doing so, the paper is divided into two parts – *first*, this paper distinguishes *Aadhaar* from other forms of government identification and highlights its novel features. These novel features are premised on the governments desire to build a 'networked platform' of governance, as opposed to a mere identification database. The researchers suggest that the rise of 'platformed government' transforms the power dynamic between citizens and the state, subjecting the former to a 'relentless gaze' directed towards achieving the 'ends of power', thus creating classic privacy concerns. We also argue for recasting the theory of privacy, *generally*, in a developing country, by finding a suitable intersection between development theory and privacy theory. Relying on Sen's capability approach, we conduct a sample privacy perception study, inquiring into how different approaches to conducting such a study affect perceptions towards privacy. In the context of ongoing constitutional litigations in India, recasting privacy theory in such terms may help the courts applying the balancing test appropriately.

PART I: AADHAAR AND THE RISE OF 'GOVERNMENT AS PLATFORM'

India's network-driven 'Unique Identification' or *Aadhaar* Project constitutes the world's largest consolidated biometric database and will – if all goes according to plan – contain the personally identifiable information of nearly 1.2 billion Indian residents. The Unique Identification Authority of India has generated more than 1 billion *Aadhaar* numbers in the span of five and a half year, and efforts are afoot to cover the entire population of the country.[1]

The first *Aadhaar* was issued in 2010 and its uptake by the Indian population has been staggering across demographics. Out of a total population of 1.2 billion, only around 230 million people remain unenrolled.[2] Of the 230 million Indians who do not have an *Aadhaar* number till now, 92%, or 217 million, are children.[3] As the table below indicates nearly all adults in India have enrolled for an *Aadhaar ID*:

AGE CATEGORY (YEARS)	Enrolment (%)
0-5	20
5-18	67
18 and Above	93

Every day, nearly 500,000 *additional* people enroll for *Aadhaar*.[4] Indeed, the rapid uptake of the *Aadhaar* initiative is not difficult to explain. Right from the outset, the government has categorically expressed its ambition to use the *Aadhaar* as the starting point for a systematic overhaul of the manner in which services, subsidies and benefits are distributed to 'deserving' citizens. *Aadhar* IDs - though not mandatory – have been linked to everything from bank accounts to diesel subsidies to essential

[1] Aadhaar Enrollment Crosses 1 Billion Mark, says Prasad, THE BUSINESS STANDARD *available at* http://www.business-standard.com/article/current-affairs/aadhaar-enrollment-crosses-1-billion-mark-ravi-shankar-prasad-116040400863_1.html (Last visited on 3rd September, 2016).
[2] UIDAI Aadhaar Data Portal *available at https://data.uidai.gov.in/uiddatacatalog/dataCatalogHome.do* (Last visited on 3rd September, 2016).
[3] *Id.*
[4] *Supra* note 1.

foodgrains. In order to incentivize speedy enrollment of the non-adults, the government is planning to link its children beneficiary schemes to *Aadhaar*.[5]

So far, 250 million bank accounts, over 71% cooking gas connections and 45% of ration cards are linked to the identification programme.[6] In this context it is easy to understand why marginalized citizens are eager to sign up for *Aadhar* and voluntarily give up their biometric data, without a complete understanding of the larger issues at stake; it promises a convenient route into the so-called 'formal' sector of the economy and legitimizes claims to government benefits, while ostensibly taking away the hegemony of the local middleman.[7]

Yet, there are tremendous sociological and legal implications associated with the rise of *Aadhar*, particularly in a country where poverty, endemic corruption and resource-leakage are a daily fact of life. The key implications arise from the fact that *Aadhaar* is a *completely novel* system of identification, without precedent anywhere else in the world. This is because the efficacy of the entire *Aadhaar* framework rests on two distinctive features:

- Aadhar promotes a fundamentally 'networked' approach to governance; and
- It goes *beyond* the mere identification of citizens for public-services, and intends to be an overarching, one-stop database, *across sectors*.

Simply put, Aadhaar is different from other identification schemes because it creates a 'networked platform' – a base upon which further products and services may be built.

Networked Governance

Let us look at each of these features individually. One of *Aadhaar's* key promises has been that the collection of vast amounts of biometric information will allow the 'real-time verification' of transactions.[8] Of course, the possibility of 'real time' identity verification is not *solely* dependent on an individual's unique *Aadhaar* number. It

[5] *Parents Struggle to Sign up Infants, Toddlers for Aadhaar as Centre Eyes 100% Enrolment by March*, SCROLL (29th August, 2016), *available at* http://scroll.in/article/814891/parents-struggle-to-sign-up-infants-toddlers-for-aadhaar-as-centre-eyes-100-enrolment-by-march (Last visited on 31st August, 2016).
[6] *Supra* note 1.
[7] *Nilekani says data is the new verification*, THE HINDU *available at* http://www.thehindu.com/todays-paper/tp-business/nilekani-says-data-is-the-new-verification/article9067516.ece (Last visited on 2nd September, 2016).
[8] *See* IN THE WAKE OF AADHAAR: THE DIGITAL ECOSYSTEM OF GOVERNANCE IN INDIA, Ashish Rajadhyaksha ed., (2013).

requires various departments of the government to be connected to the same network, and hence become 'interoperable'. The databases of these departments have traditionally existed as "*disconnected silos*", which "[make] *zeroing in on a definite identity for each citizen particularly difficult…and the lack of a unique number has given space to plenty of phantoms*".[9] A network allows accessing, collation, coordination and *comparison* of inter-sectoral databases, as well as intra-sectoral databases.[10] Indeed the possibility of authenticating and weeding out fake and duplicate identities and the claim of identifying beneficiaries or frauds – as the Aadhar claims to do – depends crucially on this ability to *compare*.

Various government departments and institutions across the world maintain population databases, but due to institutional jurisdiction and policy, or a lack of technology, these databases do not 'talk to each other'.[11] Thus, the UID is unique amongst governmental databases since it offers the technical possibility for the creation of a unitary biometric system. The UID of each individual can "*become the link number between the sectoral databases*" and thereby allow the intersectoral databases to interact depending on the agreed norms and policy decisions.[12]

Platform for Private Parties

Aadhar's distinctive 'networked' features are only exacerbated by the UIDAI's intention to allow the use of the biometric data by *private parties*. Private parties may utilize the 'data lake' created by Aadhar in one of two ways:

Firstly, if an organisation requires the identity of a person to be authenticated and it accepts *Aadhaar*, then the person in question can furnish his/her Aadhaar number. The organisation may also ask the person to furnish his/her demographic information *as well*, and take biometric tests. The captured information will be sent to the UIDAI which will authenticate the information on a 1:1 basis in 'real-time' on behalf the organisation. The UIDAI would return back an answer to the 'authentication query' in

[9] Nandan Nilekani – *Interoporerability in the Flat World*, *available at* http://www.businessgyan.com/nandan-nilekani-interoperability-flat-world (Last visited on 28th August, 2016).
[10] *The Unique Identity Project and the New 'Bureaucratic Moment' in India*, Swagato Sarkar in IN THE WAKE OF AADHAAR: THE DIGITAL ECOSYSTEM OF GOVERNANCE IN INDIA, Ashish Rajadhyaksha ed., (2013).
[11] *Id.*
[12] *Id.*

the form of 'Yes' or 'No' – on the basis of whether or not the information matched the biometric data on the database.[13]

Secondly, private parties are explicitly encouraged to build their own applications and interfaces atop the data provided by the UIDAI. That is, *Aadhaar* allows private software developers to integrate their products with information collected under the scheme. Application Programming Interfaces (APIs) allow developers to tap into the 'data stream' generated by *Aadhaar* and, consequently, use it to build their own verification platforms.[14]

This interlinking of private and public databases – particularly in the context of 'networked systems' is unprecedented in previous models of government ID. Indeed, the rise of *Aadhaar* gives rise to the risk of what Foucault terms 'Panoptic surveillance'. In the Foucaldian paradigm, control of the individual body is ideally achieved through institutions or systems that train individuals to self-discipline by directing an internalized gaze of power against themselves.[15] That is, citizens needs to feel themselves to be under constant scrutiny – even if they are not – so that they keep themselves disciplined. Foucault famously stated in order the control to individual body: "*There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by interiorising to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself*".[16] The collection of biometric information capable of tracking individual transactions within a governmental framework, raises the specter of such a gaze.

Already, applications built atop the *Aadhaar* framework reflect this sort of 'constant gaze' characteristic of the Panopticon. With the proliferation of applications built of the centralized biometric database of *Aadhaar,* to provide services relating to everything from medical records to taxi-driver verification, there is a real risk of citizens feeling the oppressive gaze of the *Aadhaar*. For instance, *Aadhaar Oauth*

[13] *Supra* note 10.
[14] India's Unique ID Project Will Open Its API, Needs Connectivity—Nandan Nilekani, Medianama *available at* http://www.medianama.com/2009/12/223-indias-unique-id-project-willopen-its-api-needs-connectivity-nandan-nilekani. (Last visited on 2nd September, 2016).
[15] Michel Foucault, *Security, Territory, Population: Lectures at the College de France 1977-1978,* (2007).
[16] *Id; See also:* Partha Chatterjee, POLITICS OF THE GOVERNED, (2004).

allows websites to use *Aadhaar* as a 'login ID"; or *Aadhaar Digital Locker* allows Internet users to store and use private documents from an online portal which is linked to *Aadhaar* verified credentials. With its links to biometric information and location services via mobile apps, citizens may be tracked and their activities logged on minute-to-minute level.[17]

Last year, a Bangalore-based start-up held the first-ever '*Aadhaar* Hackathon.' In collaboration with *Aadhaar* and the IT Industry Body National Association of Software and Services Companies (NASSCOM). More than 1,800 participants developed applications based on *Aadhaar*. In fact, the organisers even encouraged application developers to integrate biometric sensors into their applications to further integrate their products with *Aadhaar* and make them truly '*Aadhaar* enabled'.[18]

This creation of an (essentially) governmental stream of detailed biometric data system, which private parties can tap into and use to build further platforms raises grave privacy concerns. It represents a form of citizen identification unlike any other in the world. By way of an example, it may be useful to compare certain features of traditional 'Social Security Numbers' in the United States with the UID scheme:

Purpose:

SSN: The SSN serves as a number for tracking individuals in the Social Security System, and as one form (amongst others) form of identification for difference services and businesses. Alone, the SSN Card does not serve as a proof of indentity, citizenship, and it cannot be used to transact with and does not have ability to store information.[19]

UID: The *Aadhaar* number was established as a single proof of identity and address for any resident in India that can be used to authenticate the identity of an individual in transactions with organizations that have adopted the number. The scheme as been promoted as a tool for reducing fraud in the public distribution system and enabling the government to better deliver public benefits.

---

[17] *Developer built 36 apps at first ever Aadhaar hackathon*, THE BUSINESS STANDARD *available at* http://www.business-standard.com/article/technology/developers-built-36-apps-at-first-ever-aadhaar-hackathon-115011200709_1.html (Last visited on 1st September, 2016).

[18] *Id.*

[19] The United States Social Security Administration: Information *available at* https://www.ssa.gov/ssnumber/ (Last visited on 4th September, 2016).

Storage, Access and Disclosure:

SSN: The Numerical Identification System is a centralized database containing the individuals original SSN and application and any re-application for the same. All information stored in the 'Numident' is protected under the Privacy Act, 1974. Individuals may request records of their own personal information stored in the Numident. With the exception of the Department of Homeland Security and U.S Citizenship and Immigration Services, third parties may only request access to Numident records *with the consent of the concerned individual*.[20]

UID: According to the report "Analytics, Empowering Operations", *"At UIDAI, data generated at multiple sources would typically come to the CIDR (Central ID Repository), UIDAIs Data centre, through an online mechanism. There could be certain exceptional sources, like Contact centre or Resident consumer surveys, that will not feed into the Data center directly. Data is then processed in the Data Warehouse using Business Intelligence tools and converted into forms that can be accessed and shared easily."*[21] Examples of data that is stored in the CIDR include enrollments, letter delivery, authentication, processing, resident survey, training, and data from contact centres. It is unclear if organizations that authenticate individuals via the *Aadhaar* number store the number at the organizational level. Biometrics are listed as a form of sensitive personal information in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) 2011, thus if any body corporate collects biometrics with the *Aadhaar* number - the storage, access, and disclosure of this information would be protected as per the Rules, but the *Aadhaar* number is not explicitly protected. However, this issue has been addressed to some extent in the recently enacted Aadhaar Act, 2016. Ss. 28 - 33 introduce stringent measures to ensure the confidentiality of information collected under the scheme. It remains to be seen how these measures are implemented in reality.

Use by public and private entities

---

[20] The United States Social Security Administration: Consent Based Social Security Number Verification *available at* https://www.ssa.gov/cbsv/ (Last visited on 4th September, 2016).

[21] *Analytics – Empowering Operations: The UIDAI Experience,* REPORT BY THE UIDAI, PLANNING COMMISSION AND GOVERNMENT OF INDIA available at https://uidai.gov.in/images/FrontPageUpdates/uid_doc_30012012.pdf (Last visited on 21st August, 2016).

SSN: Public and private entities can request the SSN to track individuals in a system or as a form of identifying an individual. Any private business is allowed to request and use the SSN as long as the use does not violate federal or state law. Legally, an individual is only required to provide their SSN to a business if they are engaging in a transaction that requires notification to the Internal Revenue Service or the individual is initiating a transaction that is subject to federal Customer Identification Program rules. Thus, an individual can refuse to provide their SSN, but a private business can also refuse to provide a service.[22]

Any public authority requesting the SSN must provide a disclosure notice to the individual explaining if the provision of SSN is required or optional. According to the Privacy Act of 1974, no individual can be denied a government service or benefit for not providing the SSN unless Federal law specifically requires the number for a particular service.

UID: The *Aadhaar* number can be adopted by any public or private entity as a single means of identifying an individual. The UIDAI has stated that the *Aadhaar* number is not mandatory, and the Supreme Court of India has clarified that services cannot be denied on the grounds that an individual does not have an *Aadhaar* number. However, the *Aadhaar* Act passed recently in 2016, gives the power to Central and State Governments to make *Aadhaar* mandatory for any service.[23]

Therefore, as is evident, *Aadhaar* represents a drastically different identification system. It is envisaged as a 'platform' rather than a *mere* database. An 'online platform' may be defined as an undertaking which uses the Internet to enable interactions between two or more distinct but interdependent groups of users, so as to generate value for at least one of the groups. Envisaged thus, the researchers find that *Aadhaar* is, in fact, an online platform. As a centralized database geared towards identity authentication, it facilitates interactions between public service providers and the targeted beneficiaries of public welfare schemes. Moreover, *Aadhaar* also represents a platform in a more literal sense of the word – a base upon which private developers are encouraged to build their own applications. *Aadhaar* Bridge, for instance, promises '*build your apps with Aadhaar integration using one seamless*

[22] *Supra* note 19.
[23] Sec. 7, Aadhaar Act, 2016

platform'.[24] In so doing, the *Aadhaar* system represents a model – a template of sorts – of what 'government as a platform' is likely to look like.

In sum, the UID programme, with its focus on linking private, biometric information with essential public and (eventually) private services is indicative of a paradigm shift away from analogue systems of governance. It is the privacy concerns that underpin this novel system of governance that forms the focus of the next section of this paper.

PART II: DEVELOPING A FRAMEWORK FOR PRIVACY STUDIES IN DEVELOPING COUNTRIES

In India, the debates surrounding privacy often meet with the responses such as "privacy is a western notion" or "Indians don't care about privacy". The privacy skeptics argue that it is a less important problem in a developing country like India where people are still struggling with other pertinent deprivations. In some situations, these other deprivations/needs may be achieved at the cost of privacy. On the other side, the responses from the side of privacy advocates are often filled with the normative justifications for privacy, irrespective of the public perception of the same. These arguments are often rooted in the rights based justification for privacy enhancement.[25]

In the ongoing *Aadhaar* constitutional litigation in India, this narrative that shows privacy at loggerheads with other deprivations become clearly visible.[26] The Government contends that in a developing country like India, people need other public service benefits, for which identification is essential, thus claiming that the people who are not in need of the essential services are the only ones concerned about privacy.[27] Thus, privacy-skeptics in India claim that impoverished people are not even

[24] See: Aadhaar Bridge Services *available at* http://bridge.aadhaarconnect.com/ (Last visited on 25th August, 2016).
[25] Malavika Jayaram, *Aadhaar Debate: Privacy is not an Elitist Concern – It's the Only Way to Secure Equality,* SCROLL**,** (August 15, 2015) *available at* http://scroll.in/article/748043/aadhaar-debate-privacy-is-not-an-elitist-concern-its-the-only-way-to-secure-equality (last visited on 23rd August, 2016); Ashwini Kumar, Privacy, a Non-negotiable Right, THE HINDU (August 10, 2015), *available at* http://www.thehindu.com/opinion/lead/privacy-a-nonnegotiable-right/article7519148.ece (last visited on 23rd August 2016)
[26] Utkarsh Anand, Ruhi Tiwari, *Aadhaar: A Unique Problem of Identity*, THE INDIAN EXPRESS *available at* http://indianexpress.com/article/explained/simply-put-a-unique-problem-of-identity/ (last visited on 23rd August 2016)
[27] Eben Moglan & Mishi Chaudhary, *Aadhaar and the Right to Privacy*, THE HINDU *available at* http://www.thehindu.com/opinion/columns/aadhaar-and-the-right-to-privacy/article7781020.ece (last visited on 24th August 2016).

concerned about privacy-violation, leave apart *trading off* their privacy for some other good. This may have serious implications for the upcoming constitutional litigations. This is because privacy right often has to be *balanced* against some other competing value or benefit.[28] This is because the value of privacy itself is underplayed to such an extent that balancing it with other values is often of no use. Therefore, in order to conduct the balancing tests appropriately, it is important that the true value of privacy is known.

This section inquires, whether there will be any benefit to the study of privacy perception if the study is informed with the distinction between *capability* and *functionality*? The hypothesis of this section is that *while privacy may not be perceived to be an important functionality, it is an important capability*.

In the *first* part of this section, we discuss the approaches to understand privacy. In the *second* part, we briefly describe capability approach of development theory. *Thereafter*, we devise an intersection between the privacy theory and development theory in order to understand privacy better in developing country context. *Finally*, we apply this approach to conduct a sample privacy perception study to find out, if this new approach of understanding privacy assists in getting appropriate responses regarding privacy perception of people in developing countries. In order to inquire if this is true, the interview questions pertained to both – questioning right to privacy as a norm (functionality), and right to privacy as a set of harms (capability to achieve absence of these harms). The survey sample was selected keeping in mind different income backgrounds of people. This is specifically so because while the dependence on the government services is extremely high among the lower income groups, the higher income groups are not dependent excessively on the government services.

Approaches to Study Right to Privacy

A lot, though not enough, ink has been spent on the contours and notions of 'privacy'.[29] With the advent of new technologies, the scope and ambit of the right to privacy has acquired the attention of several academic commentators.[30] The

[28] *Ibid.*

[29] *See generally* Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984).

[30] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIFORNIA LAW REVIEW 1087,1130 (2002).

definitional tussles around a seemingly all-encompassing term - privacy – can largely be understood through two different approaches. One approach studies privacy as a norm – a norm that encompasses different values that are important. Under this approach, privacy is seen as an important value that needs to be protected for its own sake. Privacy is an end. It doesn't require the privacy violations to be articulated in terms of specific harms. The other approach is a harm based approach. Under this approach, privacy is not seen as an independent value, but as a means to avoid a collection of harms or problems that can be called 'privacy problems' or 'privacy harms'.[31]

While the first approach of understanding privacy theories often result into vague understandings of privacy, where it is difficult to attach any tangible value to privacy. When understood from a norm-based approach, privacy is often unsuccessful in outweighing other factors against which it is valued. Harm-based approach provides specific harms to be weighed against the other values privacy is often subordinated to.[32] We submit that this distinction is essential in understanding privacy in a developing country context.

Capability Approach

Capability approach, first propounded by Amartya Sen,[33] forms an important part of the modern development theory.[34] At its heart, capability approach relies on the distinction between capability and functionality. While functionality is defined as a state of *"beings or doings"* of a person, capability is the ability to achieve the functionalities.[35] A common example to differentiate between functionality and capability is that of starving. If a person does not consume food, the functionality is his state of being, i.e. starving. A person may starve for either of these reasons – (a)

---

[31] William L. Prosser, *Privacy*, 48 CALIFORNIA LAW REVIEW, 383 (1960).
[32] Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIVERSITY OF PENNSYLVANIA LAW REVIEW, 477 (2006).
[33] Amartya Sen, *Capability and Well-being*, in THE QUALITY OF LIFE (Nussbaum and Sen, eds., 1993); Amartya Sen, *Human Rights and Capabilities*, 6(2) JOURNAL OF HUMAN DEVELOPMENT, 151(2005).
[34] David A. Clark**,** *The Capability Approach: Its Development, Critiques and Recent Advances*, Working Paper no. 032, Global Poverty Research Group, *available at* http://www.gprg.org/pubs/workingpapers/pdfs/gprg-wps-032.pdf (last visited on August 26th, 2016); Ingrid Robeyns, *The Capability Approach: An Interdisciplinary Introduction*, INTERNATIONAL CONFERENCE ON CAPABILITY APPROACH, *available at* http://commonweb.unifr.ch/artsdean/pub/gestens/f/as/files/4760/24995_105422.pdf (last visited on August 26th, 2016).
[35] Sen (2005), *supra* note 33.

there may be lack of food; (b) he may be fasting. While one person starves due to the lack of food (and hence, the lack of capability), the other person starves out of choice, even when she was capable to having food. Therefore, though the two persons have similar functionality, i.e. their being or doing, their capabilities differ.[36]

At this juncture, it is important to locate privacy within this debate. Privacy can be a functionality – that is, if being in the state of privacy is considered a valuable end in itself. Privacy can also be a capability – that is, privacy enhances ability to achieve some other functionalities, such as security, freedom of expression, bodily integrity, dignity etc. Thus, while privacy as a functionality sees privacy as an end in itself, privacy as a capability sees privacy as a means to achieve certain functionalities. This distinction is the heart of the hypothesis of this paper.

The two dichotomies discussed above – (a) dichotomy between privacy as a norm and privacy as harms, and (b) dichotomy between privacy as a functionality and privacy as a capability – lie at the heart of this paper. The paper argues for novel way of looking at privacy issues in a developing country context - by exploring the intersection between privacy theory and development theory.

In doing so, the paper conducts a sample privacy perception study in order to demonstrate that while generally, privacy perception studies tend to inquire perception of privacy as a norm, that approach to conduct privacy perception study may not be effective in a developing country context.

Privacy Perception Studies

Privacy perception studies, though few and far between, have been conducted in various contexts and with various methodologies. The most prominent of these studies have been the ones conducted by Alan Westin.[37] Alan Westin's study has deeply influenced the existing notice-and-consent regime in the U.S.[38] In his surveys, he questioned the American people about their attitudes about technology and privacy.

---

[36] *Id.*

[37] *Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcommittee on Commerce, Trade & Consumer Protection,* 107th Congress 15 (2001) (statement of Alan F. Westin, Professor Emeritus, Columbia University, President, Privacy and American Business), *available at* https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg72825/html/CHRG-107hhrg72825.htm (last visited on August 27th, 2016).

[38] *See* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST LAW REVIEW, 261 (2014).

He divided the individuals he surveyed into three groups – privacy fundamentalists, privacy pragmatists, and privacy unconcerned.[39] His survey classified most of the American respondents as 'privacy pragmatists', i.e. people who favour voluntary standards and consumer choice over legislation and government interference, unless voluntary means are not able to do enough.[40]

The critics of this approach argue that the responses of Westin's surveys may have been misguided and counterproductive due to the lack of consumer awareness about the uses of the information collected and the possible protections against it. In fact, the critics argued that some of the people who initially identified themselves as privacy pragmatists found themselves to be privacy fundamentalists when they are appropriately informed about the problems with data collection and the safeguards surrounding the usage of their data.[41]

While lack of awareness definitely undermines the appropriateness of privacy perception tests, as with Westin's framework, there may be other factors that equally undermine the results of privacy perception tests. It is submitted that these studies presume privacy to be a functionality, instead of a capability to achieve other functionalities. Functionality-based understanding of privacy is analogous to norm-based approach to understand privacy theory – i.e. privacy is consider as an independent norm that has to be achieved for its own sake. This way, privacy becomes a desirable act of *being* and hence, a functionality in itself. The establishment and acceptance of a particular norm in a society is a deep cultural and political process. However, privacy's importance is not merely cultural or political, but there may be tangible, clearly visible harms arising due its absence. Therefore, even if a value is not considered as a norm, it may be considered important for its ability of preventing those harms.

However, limiting privacy studies to merely norms or functionalities, may not give us a complete picture of privacy perception. It is this conceptual problem in arriving at privacy perceptions that gives rise to claims that negate privacy as a norm in India and in many other developing countries. These claims, in their simplistic forms, are often manifested in responses such as "privacy is a western notion" or "Indians don't care

[39] *Supra* note 37.
[40] *Id.*
[41] Hoofnagle & Urban, *supra* note 38, at 305.

about privacy". Thus, it is submitted that the claims negating the requirement of a constitutional right to privacy or a privacy legislation, are more often than not, rooted in our functionality-based understanding of privacy.

Earlier Privacy Perception Studies in India

While generally there is dearth of privacy perception studies in India, there is one conducted in 2004 that provides insights into consumer privacy.[42] The responses elicited in that study manifest the functionality-based approach to understand privacy. The result of this study clearly showed that the sample from India did not consider privacy to be an important norm. The hazard of these studies that adopt functionality-based approach to privacy is that they only show if people consider privacy to be a desirable state of being or a norm. It does not inform us if privacy is essential to achieve certain other states of being that may be considered desirable by people.

An appropriate privacy perception cannot be carried in terms of a single question that asks the populace if they value the privacy being violated by *Aadhaar* scheme. As opposed to this kind of privacy perception, this study aims at conducting a detailed study, one that locates at the interface between privacy theory and development theory. Therefore, functionality-based privacy perception studies do not adequately inform us about the need for privacy protection. Relying on this intersection between privacy theory and development theory, we analyse the privacy perception with respect to *Aadhaar* project.

This does not mean that this paper seeks to prove that privacy is not a norm in India. Whether privacy is a norm or not in India has to be proved independently and cannot be simply asserted. However, this paper seeks to evaluate the impact of the approach we adopt for understanding privacy on outcomes of privacy perception studies. The two approaches that this paper compares are, functionality-based approach of privacy, and capability-based approach of privacy

Methodology

Theoretical Framework

[42] Ponnurangam Kumaraguru, Lorrie Faith Cranor & Elaine Newton, *Privacy Perceptions in India and the United States: An Interview Study* (2004), *available at* http://precog.iiitd.edu.in/Publications_files/tprc_2005_pk_lc_en.pdf (last visited on August 24th, 2016).

A capability needs to have certain functionalities, i.e. a capability is always towards the end of achieving certain functionalities. When it comes to privacy, the functionalities should be understood in terms of *'absence of harms'* that privacy violation may cause. For the purpose of this study, we will call them 'privacy harms'. Therefore, if privacy perception study shows that absence of certain privacy harms (functionalities), are considered to be valuable and desirable by the people, privacy is required as a capability to achieve the set of desired functionality. In that case, privacy protection is required because it is an essential ability to achieve the desired set of functionalities. On the other hand, if those functionalities are not considered to be desirable, privacy is not even a capability. In that case, the people may not desire privacy protection.

For determining essential functionalities or privacy harms, we rely on Solove's framework of privacy harms. Solove in his masterpiece, *A Taxonomy of Privacy*, laid down a list of privacy harms broadly classified into information collection harms, information processing harms, information dissemination harms, and invasion harms. Though there have been other classification of harms such as that of William Prosser,[43] Solove's list of harms is the most comprehensive one. Therefore, in this study, we will consider the absence of these harms as functionalities.

The perception tests was carried out in the form of semi-structured interviews of 40 interviewees. The essential qualifications for all the interviewees were – (a) they have already enrolled for and already posses *Aadhaar* number, and (b) they have used the *Aadhaar* number at least once.

Profile of the respondents

- To strike the gender balance, the respondents were chosen in such a way that both male and female respondents are equal in number.

[43] Prosser, *supra* note 31, at 389. According to Prosser, the privacy harms can be classified into four classes: "1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; 2. Public disclosure of embarrassing private facts about the plaintiff; 3. Publicity which places the plaintiff in a false light in the public eye; and 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness"

- While 30 respondents belonged to lower income groups, and aged more than 40 (Group A), 10 respondents belonged to higher income groups and the age group of 20-30 (Group B). This combination was deliberately chosen to inquire if the class-situatedness and age affects the perception of privacy. Within these two groups, there are equal members of both the sexes. Overall, the interviewees belonged to 7 different states of India.

- The interviewees consisted from various backgrounds – students, construction workers, sweepers, shopkeepers, security guards, cab/auto drivers, and engineers.

Unstructured Interviews

Instead of following a set questionnaire of 'Yes' or 'No' questions, we have conducted unstructured interviews. The interviewees were informed beforehand that they are being interviewed for a study on *Aadhaar*, but not about the arguments or the hypothesis of the paper, so that their answers are not affected by it.

Interview Questions

- The interview questions were divided into three parts – (a) introductory questions; (b) questions with the object of inquiring if they consider privacy to be an important functionality, and (c) questions with the object of inquiring if they consider *absence of privacy harms* to be important functionalities (and hence, privacy itself as an important capability).

- Introductory questions included question like - *Do you use Aadhaar for any services?; If not, why have you enrolled for the same?; What have you heard about Aadhaar scheme?; Do you think Aadhaar has benefited you till now in a way different from other identity cards have?; What will be the problems in its implementation according to you?*

- Questions about privacy as functionality were direct questions about keeping information private. The objective was to inquire if the respondents considered giving away private information inherently problematic. The specific questions were – *Do you think right to privacy is important?; Do you think it is problematic if government*

takes your fingerprints and iris scan?; Do you think it is problematic if government uses it for multiple purposes?

- The most important questions, were however, the questions that were aimed at inquiring, whether absence of privacy harms is considered to be important functionalities (or, if privacy is an important capability). These questions were framed based on Solove's proposed framework. Solove's privacy harm classification is quite comprehensive, and hence, all privacy harms given by him are not applicable in the case of *Aadhaar*. While some privacy harms in Solove's classification are not applicable to *Aadhaar*, some harms clearly are. Therefore, the interview questions were also limited to those harms – surveillance, aggregation, insecurity, and disclosure.

Analysis of the Interview Answers

Functionality-based understanding of Privacy

The questions pertaining to functionality were aimed at inquiring if the respondents considered privacy as a desirable state of *being* (and hence, a desirable functionality). The responses have not been uniform. All the 10 members that belonged to Group B accepted privacy to be an important state of being. While all of them accepted that right to privacy is important, as it is clear from their responses like *"Asking me give my fingerprints is like asking me to give a part of my body"*, they also qualified their acceptance of right to privacy, stating *"it is not an absolute right…privacy may have to be traded sometimes based on the other considerations"*. While not all of them identified themselves to be privacy fundamentalists, they recognized that privacy has to be taken very seriously in the balancing exercise. Only 2 out of 30 respondents in Group A identified privacy as an important functionality, manifested in responses such as *"yes, these are my fingerprints. I should not be forced to give them"*, and *"fingerprints are like my phone no…they are private details"*. However, the other 28 respondents in Group A did not consider privacy as a desirable functionality. All of them directly rejected the proposition *"right to privacy is important"*. They did not consider privacy protection from fingerprints collection in itself an important functionality. As per their perception, their well-being will not be hampered by the Government's collection of their fingerprints, iris scan, and other personal data. The responses were common and repetitive – *"There is no harm in collecting your*

fingerprints or whatever data", and *"it will make police's job easier, it's good"*. On being asked about the requirement of right to privacy or a law governing private data, the responses were *"what is private about your details! It is not a secret"*. Right to privacy was mostly understood as a right to hide things, wherein some reacted to it as "why to give opportunity to these criminals to hide stuff?" The responses elicited an understanding that broadly, the people in Group A do not understand right to privacy as a norm.

The question that arises is, even if people in Group A do not consider privacy to be an important norm, whether that is sufficient to negate the need for privacy regulation or a right to privacy? We submit that it is not true. This rejection by Group A is only a rejection of particular approach to understanding privacy – functionality based approach. Therefore, in the next section, we inquire if these same people will adopt the capability based approach to privacy. In order to test if the hypothesis is true, we will analyse the responses of *only* those 28 respondents (out of total 40) who did not consider privacy to be an important functionality.

Capability-based understanding of Privacy

In order to inquire if privacy is perceived to be an important capability, one has to inquire if the harms that may be possibly caused by *Aadhaar* scheme are perceived to be important harms. In that way, privacy becomes an important capability to achieve the absence of those harms. Following Solove's framework, we divide our capability-based approach of privacy perception into four parts – based on different qualification of harms.

(i) Harms Relating to Information Collection: Surveillance

The specific relevant harm pertaining to information collection is that of 'surveillance'. We asked our questions as specific examples of government surveillance over the activities of individual citizens such as - what if the government keeps a track of the activities pertaining to your visit to banks, hospitals, railway stations, etc.? Would you participate in a protest against the government if the government could easily identify you? Are you fine with government collecting data without specifying any purpose? Now that the government has so much of the information, do you feel threatened of the government's powers?

Based on our analysis of their descriptive responses, while 10 out of the 28 respondents in Group A perceived this is to be a problem, the other 18 in this group did not perceive mere government surveillance to be an important problem. The change in privacy perception of these 10 respondents, who did not consider privacy to be an important functionality, is a clear demonstration of the proposition that absence of surveillance harms is a desirable functionality for these respondents, even if privacy *per se* is not. However, since privacy is a necessary capability to achieve absence of surveillance harm, their overall perception towards privacy changes when asked the right questions.

At the same time, it can be concluded that absence of surveillance is not an essential functionality for majority of people in Group A. However, surveillance is not the only privacy harm relevant to *Aadhaar*.

(ii) Harms Pertaining to Information Processing: Aggregation and Insecurity

There can be multiple harms under the broad umbrella of information processing harms that can be caused by *Aadhaar* – such as aggregation and insecurity. Since these harms are related, the questions posed refer to these harms collectively – do you think if single identification is used for all the purposes, instead of individual identification tools? Do you think it is problematic that all your services, activities, and claims may be dependent on a single source of identification? Out of 28 respondents, 18 accepted it to be an important harm. This was manifested in responses such as *"yes, I did not think of it. So, if there is some problem in my Aadhaar number, all of my activities may be affected"*; and *"they may block all the services if I default my payment in one of the services"*. Therefore, it is clear that aggregation is considered to be important privacy harm by 18 people who had earlier negated the importance of privacy as a functionality. This further shows how privacy perception results may differ merely on the basis of the approach that is adopted.

Similarly, for the harm of information insecurity, we asked the questions – Do you think it is problematic if someone commits an identity theft on you? Do you think it is important that the system collecting your data should be fully protective of your identity related information? What if the information fell into the hands of wrong people? What if they steal your identity or hack your finger prints/iris scan? Do you think it is problematic if the data is lost or *Aadhaar* becomes non-functional, even if it

is for a short while? Out of 28 respondents, 25 considered this to be an important harm. Therefore, there are 25 persons who did not consider privacy to be an important norm, perceive information insecurity to be an important harm. Therefore, information security is also an important functionality that privacy is an essential capability for.

(iii) Harms Pertaining to Information Dissemination: Disclosure

Harms pertaining to information dissemination are the biggest category of privacy harms. This umbrella category encompasses multiple privacy harms. The harms specifically relevant to *Aadhaar* scheme are disclosure and distortion.

"Disclosure occurs when certain true information about a person is revealed to others."[44] The risk of disclosure can inhibit people from engaging in transactions or associating with others. Disclosure also makes people vulnerable to certain attacks or threats. Relying on these rationales of disclosure harm, the questions that were raised - are you fine if the information stored in the government database is leaked and several other people including your employer come to know about your visits, etc.? What do you think if your information regarding your visits is disclosed to private parties? What do you think if the Government uses a mass-chunk of data and makes mistakes in analyzing in important decisions about public service provision? What do you think about the possibility of faking fingerprints, in case some researchers claim that it is very easy to distort the fingerprints? What do you think of the possibility of someone changing information about your activities in the government database? What do you think about Government drawing wrong conclusions based on your use of *Aadhaar* for during visits to different places?

Based on the analysis of the responses to these subjective questions posed, out of 28 respondents, 25 accepted absence of disclosure harms to be an important functionality. Since privacy is an essential capability to achieve this functionality, they have also accepted the value of privacy as a capability.

Conclusion

[44] Solove, *supra* note 32, at 529.

There are these 28 people who believed that privacy is not an important functionality. However, when questioned in terms of absence of privacy harms for which privacy is an important capability to achieve, the privacy perception changed substantially. The below table shows how those 28 people responded to different harms:

Harms	**Surveillance**	**Aggregation**	**Information Insecurity**	**Disclosure**
No. of respondents perceived it be a harm (total 28)	**10**	**18**	**25**	**26**

In total, there were only 2 respondents who considered privacy to be neither an important functionality, nor an important capability. Further, there were 10 respondents who affirmed all the four harms to be important harms, and 19 affirmed that at least three of the four harms listed above are pertinent harms. The study teaches us that almost every respondent who did not consider to be an important functionality/norm, considered it be an important capability.

CONCLUSION

It is the our central argument throughout this paper, that the Aadhaar programme, as it currently stands, represents a paradigm shift away from analogue systems of governance. It represents the rise of 'platformed governance' and presents a template of the manner in which technology is likely to recast the manner in which citizens interact and makes claims upon the government. Moreover, by linking public and private service providers within the Aadhaar framework, the UID programme also fosters a Foucaldian Panopticon – with grave consequence for privacy within the Indian democractic framework. Perhaps this papers most salient insights are presented in Part II – where we sought to develop a theoretical framework within which privacy rights ought to be conceptualized in developing countries.

In the ongoing constitutional debates in India on right to privacy, and specifically in the context of ongoing litigation on validity of *Aadhaar*, the claims ignoring privacy as an "un-Indian" concern or a "western notion" are abound. We conclude that this is essentially a result of our conceptualization of privacy being tied to the *state of being in privacy* – that of functionality, rather than understanding privacy as a capability to achieve the absence of certain privacy harms.

Further, this paper does *not* argue that in all the cases concerning privacy violation, privacy should *always* triumph over other values that may weigh against privacy. Instead, we recognise that even judicial determination of rightness or wrongness of a privacy violation is ultimately a balancing exercise – where right to privacy is often balanced against some other values, such as national security, efficiency, etc. Therefore, we argue that though privacy may be outweighed by other values at stake (for instance, public services efficiency in *Aadhaar*'s case), due weightage should be given to privacy in this exercise of balancing.

What our study suggests is that in the specific case of *Aadhaar*, the privacy harms posed are perceived to be dangerous by most of the respondents, and hence, privacy may outweigh other competing values. However, our study has limitations in the form of limited sample size – we believe the conclusions we arrive at may be generalized.