PRIVACY AND THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL: LEAVING MUCH TO THE IMAGINATION

*Amba Uttara Kak and Swati Malik**

The National Identification Authority of India Bill ('the Bill') *leaves many things unsaid. It has delegated most key areas relating to the institution of the system of unique identification* ('UID') *numbers (officially known as 'aadhar' numbers) to rules to be framed by the authority subsequently. Its definitions are almost all open-ended. Right from the public announcement of the project, to the drafting of the Bill, the furore over the introduction of this system of identification has only been growing. Those critical, as well as those in support of the project have based their opinions on the various hypothetical outcomes they believe this project could have on welfare schemes, privacy of individuals and indeed, the nature of governance in India. Such critiques are based on the ambiguities in the law and a suspicion that such ambiguity will prove to be particularly dangerous with respect to information privacy. In this context we will examine the exact contours of what this draft legislation does say, and the system of identification it envisions. Whether inevitable privacy concerns arising out of such a data collection excercise have been dealt with in a meaningful and comprehensive manner and furthermore, the manner in which the national security rationale has manifested itself in the project as well as the legislation.*

I. INTRODUCTION

The Bill is slated to be introduced in Parliament in the Winter Session of 2010.[1] Its stated purpose is for provision of identification numbers for individuals residing in India, corresponding with collection of biometric and identity information of such individuals to ensure every resident can avail of public welfare

* 3rd Year and 1st Year students respectively, The West Bengal National University of Juridical Sciences, Kolkata. The authors would like to thank Professor Phillip Dann, Dr.iur., LL.M., Max Planck Institute for Comparative Public Law and International Law, for his valuable insights regarding unique identification project in other jurisdictions. We thank Mr. T. Prashanth Reddy for providing initial guidance for certain ideas developed in this article. We also thank Mr.N. Sai Vinod, 3rd year student, West Bengal National University of Juridical Sciences, Kolkata for providing valuable inputs and suggestions during research for this paper.

[1] Reporter, Identification Authority Bill Gets Cabinet Approval, The Business Standard (New Delhi) September 25, 2010.

services and benefits.[2] Although this Bill was introduced as recently as August 2010, the Unique Identification Authority of India ('UIDAI') was set up directly under the Planning Commission in February, 2009. It was made responsible for development and implementation of the technical, legal and institutional infrastructure necessary for a system of identification numbers.[3] A few months later, the Cabinet itself appointed Mr. Nandan Nilekani, recognized as one of India's most successful software entrepreneurs in the information technology sector, as the Chairman of the project, the first to have the status/rank of a Cabinet Minister. The project was off to a very hyped start and less than three months later, the design document of the UIDAI project was leaked and found itself in the public domain.[4] The sheer scale of the project invited curiosity, but much was left unknown. The Bill was finally published on the official website as late as August 2010 and a mere two week window was allowed for suggestions from the public. Prior to this, the implementation of the project was well under way; an interim budget of 100 crore rupees had been earmarked in 2009, tenders released and several agreements with the proposed Registrars such as State Governments, LIC, Ministry of Rural Development etc. had already been signed.[5] Therefore, much before the Bill has been introduced in Parliament, the first UID number was issued to an individual at the national launch of the project in Tembhli, Rajasthan in September 2010.[6] Subsequently, issuing of numbers has ensued in other regions.[7] Given that the UIDAI was set up as a purely executive body, it could be argued that this project did not necessarily require legislative sanction and the reason for the Bill is essentially to give the UIDAI statutory sanction, and thereby, increased access to funds. Given that this Bill has come out so late in the process, another major concern is the lack of any public consultation or discussion in Parliament regarding the scope and implementation of this project.[8] It is important

---

2 The National Identification Authority Bill of India, 2010, Preamble, available at http://www.prsindia.org/uploads/media/TheNationalIdentificationAuthorityofIndiaBill2010.pdf (Last visited on November 1, 2010).

3 Unique Identification Authority of India, Mandates and Objectives, available at http://uidai.gov.in/index.php?option=com_content&view=article&id=141&Itemid=164 (Last visited on November 1, 2010).

4 Gideon Swift, *Confidential Plans for 1.2 Billion ID Cards: Creating a Unique ID for Every Resident in India*, November 13, 2009, available at http://www.the-gates-of-hell.com/confidential-plans-for-1-2-billion-id-cards-creating-a-unique-id-for-every-resident-in-india/ (Last visited on November 1, 2010), cf. Ruchi Gupta, *Justifying the UIDAI: A Case of PR over Substance?,* ECONOMIC AND POLITICAL WEEKLY (Mumbai), October 2, 2010, 136.

5 *See* NetIndian News Network, *LIC Becomes First Institutional Partner in UID Project,* June 6, 2010, available at http://netindian.in/news/2010/06/09/0006786/lic-becomes-first-institutional-partner-uid-project (Last visited on November 1, 2010).

6 Ambika Pandit, *UID Gives Identity, Bank Account to 27 Homeless*, THE TIMES OF INDIA (New Delhi) November 29, 2010, available at http://timesofindia.indiatimes.com/city/delhi/-UID-gives-identity-bank-account-to-27-homeless/articleshow/7007753.cms#ixzz1AMLlamHO (Last visited on January 7, 2011).

7 Official Press Release*, National launch of the Aadhaar Project*, available at http://uidai.gov.in/index.php?option=com_content&view=article&id=179&Itemid=220 (Last visited on November 20, 2010).

to investigate this claim, as it sheds light on public attitudes towards participation in the legislative process and the issue of privacy. The publicity for the UID project purports every citizen to be a stakeholder; yet in reality many argue that this project has not been nearly 'consultative' enough. The official annual budget for the year 2010-2011 is Rs.1.9 crore, whereas public estimates of the entire project cost range widely between Rs. 70,000 crores to Rs. 1,50,000 crores.[9] Given the huge costs, and the self proclaimed mandate of 'universal inclusion', the sanction of the project design and budget for the project without public engagement or cost-benefit analysis has prejudiced public faith in this project considerably. In Part II of this article, we will examine the nature of biometric data collection programs in India in the past, specifically looking into the public engagement with such programs on the issue of privacy. Part III will analyze two important definitions provided for in the Bill, namely, the kind of information to be collected and the role of 'Registrars' who will collect such information. These definitions are critical to understanding the scheme of the project as outlined in the Bill. In Part IV, we provide a descriptive analysis of the step by step scheme of UID which has been provided for in the Act, as well as pin point the various loopholes. Finally, in Part V we examine the privacy concerns emanating out of data collection of such. The focus is on the dangers of not specifying which bodies may request authentication, as well as concerns of profiling and tracking of individuals. Part VI will explore the lesser publicized rationale behind the Bill of tightening national security, the connection of the UID with several security programs and the suspicion surrounding this link.

II. BIOMETRIC DATA COLLECTION PROGRAMS IN THE PAST

This article will concentrate on an analysis of the draft legislation for the UID project, but we will begin by introducing certain similar biometric data collection programmes in the past in India which have proceeded without corresponding laws. An analysis on the same has been conspicuously absent from all public discussion on this project. In a debate proceeding from hypothetical claims, it is pertinent to look into such programmes to ascertain actual experience.

---

[8] *No UID Till Complete Transparency, Accountability and People's Participation: A Public Campaign*, The Centre for Internet And Society, New Delhi, August 2010, available at http://www.cis-india.org/events/no-uid-till-complete-transparency-accountability-and-peoples-participation-a-public-campaign/?searchterm=%20uid (Last visited on November 20, 2010);Usha Ramanathan, *A Unique Identity Bill*, Economic and Political Weekly (Mumbai), July 24, 2010, 10-14; Ruchi Gupta, *Justifying the UIDAI: A Case of PR over Substance?,* Economic and Political Weekly (Mumbai), October 2, 2010, 135-136.

[9] Correspondent, *Citizen IDs to cost Rs 1.5 lakh crore*, The Times of India (New Delhi), June 26, 2009; Praful Bidwai, *Questionable Lin*k, Frontline (New Delhi), June 5-18, 2010. For official estimates, *see* Unique Identification Authority of India, Annual Budget, available at http://uidai.gov.in/index.php?option=com_content&view=article&id=147&Itemid=155 (Last visited on November 1, 2010).

In May 2010, it was reported that the Andhra Pradesh State Government had collected biometric information resulting in an iris scan database of approximately 5.8 crore people.[10] The collection of such information took about 5 years, and was followed by the creation of an online database for ration cards. In the process of de-duplication, 1.1 crore ration cards were found to be bogus.[11] The Andhra Pradesh Civil Supplies Department, in charge of this programme, stated that consolidation of these databases for various schemes such as Public Distribution System, National Rural Employment Guarantee Scheme, Pension, etc. into a single integrated database was the desired goal.[12] The Karnataka State Government also began issuing biometric ration cards based on a 2006 survey of citizens below the poverty line. Here, collection involved fingerprints and photographs.[13] An official figure of 5.56 lakh biometric ration cards were meted out to BPL families. In fact, the Tamil Nadu State Government, is set to issue biometric ration cards to 1.97 crore ration card holders in a project which should be completed by June 2011.[14] The biometric information would include iris scans and fingerprints along with photographs of the heads of families.

State Governments have gone about these programs without any sign of legislative regulation or sanction. Given the sensitive nature of biometric information, it is indeed worrying that there was no law preventing the sharing of this biometric information with other state agencies such as the police, for example. Even so, there does not appear to have been any public dissent over the collection of biometric data for the provision of services. In this regard, the raging public debate over the effect of the UID project on privacy of individuals is a welcome change, as is the fact that this Bill seems to be an attempt at regulation of the same.

To the extent that the UIDAI has pegged de-duplication and consolidation of databases as one of the major potential benefits of the project,[15] the statistics from similar projects in the abovementioned states are a strong argument for the fact that biometric identification is in fact workable in India. However, one mustn't forget the reasons that the UID project itself emphasises to

---

[10] The Hindu Business Line, *Ration Cards: 1.1 Crore Biometric Samples Found to be Duplicate*, THE HINDU BUSINESS LINE, May 13, 2010, available at http://www.thehindubusinessline.com/2010/05/13/stories/2010051351831900.htm (Last visited on November 21, 2010).

[11] *Id.*

[12] *See* K. Raju & M. Padma, Department of Rural Development, in R K Bagga, Piyush Gupta (eds.) TRANSFORMING GOVERNMENT – EGOVERNMENT INITIATIVES IN INDIA, 2009, available at http://www.nisg.org/knowledgecenter_docs/B02020001.pdf?PHPSESSID=15bff8502a0710f6c6d46c8ad895dfc6 (Last visited on November 21, 2010).

[13] Shankar Bennur, *Mysore: Biometric Ration Cards Issued to 5.56 Lakh Beneficiaries*, THE HINDU (New Delhi) July 17, 2010, available at http://www.hindu.com/2010/07/17/stories/2010071752020300.htm (Last visited on January 7, 2011).

[14] Times Chennai, *Centre's Nod for Bio Metric Ration Cards*, TIMES CHENNAI, July 26, 2010, available at http://www.timeschennai.com/index.php?mod=article&cat= Chennai& article=5871 (Last visited on November 21, 2010).

[15] *See* Presentations by UIDAI, *What is Unique About India's UID?*, available at http://uidai.gov.in/images/FrontPageUpdates/tampa/WhatisUniqueaboutIndiaUIDProgram.pdf (Last visited on November 21, 2010).

justify its 'uniqueness'. It is still distinct from these earlier programmes as it provides identification to the individual, and not the household. Moreover, the use of a ration card is by the household to gain access to entitlement whereas the UID system would give the individual a number on the basis of which, external agencies could verify information they possess about the individual. Although lack of identity proof is touted as the reason for this project, there appears no statistics in any official documents or statements as to the extent of the population that lacks such proof. Ration cards are the most prominent form of identification in India, even in the most remote rural areas. While it is true that developmental schemes such as the NREGA, and PDS faced hindrances due to identification of beneficiaries, it was not the *existence* of 'identification proof' that posed a problem, as much as fraud, collusion between middlemen and labourers etc. that did.[16] Hence, to the extent that biometric data can ensure de-duplication of the database, it is acceptable that a UID number could effectively address the problem of fraud in such schemes. However, this would require universal enrolment, and compulsory enrolment is catgorically *not* a requirement of the UIDIA.[17] It could be argued that introducing biometrics in ration cards would serve the same purpose, and therefore there is no need for the UID as a whole new identity for people. Further, although its mandate stresses on its use for access to social welfare benefits, it is clear that the UID database will have several other uses which justify its 'uniqueness'. The UIDAI has explained 'financial inclusivity' to be one, i.e. that poor residents will be able to easily establish their identity to banks.[18] These 'several other uses' have also been inferred from a reading of the Bill itself, such as 'national security' although discussion on this aspect of the project has been absent from the official publicity of the project. In fact, it is with such 'other uses', that the skepticism surrounding the Bill originates.

The Preamble of the Bill provides for the establishment of the Authority and provision of 'aadhar' numbers in order to "facilitate access to benefits and services to such individuals to which they are entitled" (emphasis supplied). The UIDAI does not make any claims on providing rights, and has specifically stated that "UID number will only guarantee identity, not rights, benefits or entitlements".[19] The Preamble states that such numbers shall apply to "individuals residing in India and to certain other classes of individuals" (emphasis supplied). Although the use of the UID seems to be directed at residence and not citizenship, this general term leaves room for doubt. This ambiguity is apparent in the stated purpose as well, where it states "and for matters connected therewith or incidental

---

[16] *See* Reetika Khera, *Not all that unique*, The Hindustan Times (New Delhi) August 30, 2010, available at http://www.hindustantimes.com/Not-all-that-unique/Article1-593541.aspx (Last visited on January 7, 2011).

[17] *Id*.

[18] *See Aadhaar May Be Sufficient to Open Bank Account,* Business Standard (Bangalore) September 7, 2010, available at http://www.business-standard.com/india/news/aadhaar-may-be-sufficient-to-open-bank-account/407247/ (Last visited on November 1, 2010).

[19] UIDAI, *Creating a Unique Identity Number for Every Resident in India*, Working Paper, Unique Identification Authority of India, (2009); Praful Bidwai, *supra* note 9.

thereto". Through the course of this article, we will discover that the matters connected to the UID are manifold, but not always incidental to access to benefits and services, such as national security.

The structure of the Bill may be summarized as follows. The introductory chapter provides the important definitions of terms used in the Bill. The second outlines the properties and authentication purpose of 'aadhar' numbers as well as provides for special measures to issue 'aadhar' numbers to certain categories of people such as the elderly, disabled, migrant workers, unorganized workers etc. Chapter III establishes the National Identity Authority of India, the position of Chairman, members, officers and lists its powers and functions. Chapter IV deals with the finances of the UIDAI from grants and funds to accounts and annual audits. Next, the composition of an Identity Review Committee is set out, along with its powers to review the working of the 'aadhar' number system and the usage pattern of the same. Chapter VI provides for the protection of information held with the Central Identities Data Repository ('CIDR') whereas Chapter VII lists the offences, and corresponding penalties for impersonation, and unauthorized disclosure or access to such information. The final part deals with several miscellaneous provisions, such as the power of the Authority to delegate its functions, and the central government's power to make rules, to name a few.

III. IMPORTANT DEFINITIONS

A. INFORMATION

§3(1) entitles every 'resident' to an 'aadhar' number on providing his/her demographic information, and his/her biometric information. This implies that it is residence, and not citizenship, that is the criteria for obtaining this number. Further, §6 provides that authentication is not proof of citizenship or domicile and will not qualify as substantive proof of nationality or domicile.[20] On the question of whether 'resident' includes illegal migrants or visitors with visas to India, the UIDAI maintained that "all residents who are in India and may want to avail services" can obtain UID numbers.[21] They have stated that deciding on the legal status of immigrants is beyond their jurisdiction, and the role of other government departments.[22]

The definition of information sought to be collected requires scrutiny. The two categories of information are defined in §2. Biometric information is

---

[20] Unlike this system, Germany, Singapore and Spain include nationality as a criterion of information under their National IDs.

[21] UIDAI, *Frequently Asked Questions: Residents and Unique Identity*, available at http://uidai.gov.in/index.php?option=com_fsf&view=faq&Itemid=206&catid=3 (Last visited on November 1, 2010).

[22] *Id.*

defined as simply the biological attributes of an individual.[23] The specifics of the type of biometrics have been left to regulations to be specified by the UIDAI. Currently, the collection of biometric data for the project includes iris scans and fingerprints. Demographic information is defined, but using the words "includes such information" which demonstrates that the list is not exhaustive and open to additions.[24] Such mandatory information would relate to name, age, gender and address of the individual. §54(2)(a) specifically provides the authority with the power to make regulations for biometric and demographic information. It is argued by civil society organizations that the information to be collected is important enough to be made part of the Central Governments rule-making function under §53 instead of bestowing such authority on the UIDAI itself.[25] This argument rests on certain assumptions about the accountability of these two entities. Even so, the argument remains that the 'kind' of information collected is sensitive in terms of its potential to affect the privacy of individuals if misused.

To the extent that an individual's name and corresponding address may be used in a manner contrary to his privacy, even such 'basic' information is regarded as sensitive.[26] The degrees of sensitivity however, also depend on social and cultural contexts. The Bill recognizes this 'sensitivity' of information to the extent that it expressly prohibits collection of information relating to caste, income, race, religion, caste, tribe, ethnicity, language, income or health. Interestingly, the Union Cabinet recently approved the inclusion of caste in the Census 2011.[27] A full-fledged caste census is to begin once the current population enumeration ends. Those who raise privacy concerns about the UID project with respect to the information sought to be collected differentiate the Census on grounds of legal safeguards. It is argued that the Census Act, 1948 protects confidentiality by an express provision which categorically states that information collected is *not open to inspection nor admissible in evidence*. (emphasis supplied).[28] Such a privacy safeguard is not part of the Bill, which only penalizes the 'unauthorized' disclosure by an employee of the UIDAI, and not disclosure *per se*. Unlike the census, the Bill in fact explicitly authorizes disclosure of information pursuant to an order of a competent Court or by an executive order under certain circumstances.[29]

---

[23] §2(e), The National Identification Authority Bill of India, 2010, available at http://www.prsindia.org/uploads/media/TheNationalIdentificationAuthorityofIndiaBill2010.pdf (Last visited on November 1, 2010) ('the Bill').

[24] §2(h), the Bill.

[25] Centre for Internet and Society, *Feedback on the UID Bill*, available at http://www.cis-india.org/advocacy/igov/letter-to-uid-authority/view?searchterm=letter%20to%20uid%20authority (Last visited on November 1, 2010).

[26] §43A of the Information Technology Act, 2000 uses the term 'sensitive personal data' however, it delegates the definition of this term to the Central Government. Till date, there has been no clarification on the meaning of this term and what it can entail.

[27] CNN IBN, *Cabinet Approves Caste Census from 2011*, September 9, 2010, available at http://ibnlive.in.com/news/cabinet-approves-inclusion-of-caste-in-census/130620-37-64.html (Last visited November 21st 2010).

[28] §15, Census Act, 1948.

[29] §33, the Bill.

The Malaysian national ID card experience reveals important insights regarding the harms out of sensitive personal data collection. In 2001, the Malaysian government introduced a national smart card called the MyKad.[30] The MyKad serves as a national ID, driving licence, provides passport and health information. Several other applications such as ATM access and even credit card use have been purported for future use. Apart from basic personal information such as name, gender and address, the personal demographic information collected for the card also includes race, citizenship, religion, health, marital status, polling station code and date of registration as a voter, code for criminal record and restricted residence and demerit points. However, there has been an overwhelming concern that such a comprehensive dossier of personal information can result in the 'authorized' use of such information for profiling individuals. This is known as 'data surveillance' and has been described as the systematic use of personal data systems to enable monitoring of all actions and communications of individuals.[31] Information relating to race, religion, HIV status, past criminal record and marital status is 'sensitive' in that enforcement agencies are better equipped to target certain categories of people by their access to these respective databases. In Malaysia, only those whose stated religion is Islam have the word 'ISLAM' printed on their card itself, although this has been heavily opposed given that it is discriminatory to other religions.[32] Further, the danger with health information, or marital status in particular, is that it allows the government to profile and discriminate against citizens who they categorize as 'non-conformist' or 'alternative'.[33] The inclusion of voting information has led to increasing the potential of the government to monitor, track and link voting patterns of an individual. The 'violent' potential of information data bases were exposed even in India, in the Gujarat riots, where it was voter lists that enabled the organization of collective violence.[34] These examples highlight that the mere collection of information is far from benign; it can be put to harmful uses and serve the interests of the government/enforcement agencies/third parties as opposed to those of the individuals by enabling atrocities to be committed on them.

Entitlement to welfare programs is often based on conditions of caste and income. Therefore, it may be argued that including information relating to these would be in tune with the purpose of the UID project to increase access to such welfare programs. Moreover, bogus certificates for caste, income have long

---

[30] Mathews Thomas, *Is Malaysia's MyKad the 'One Card to Rule Them All'? The Urgent Need to Develop a Proper Legal Framework for the Protection of Personal Information in Malaysia*, 28 MELB. U. L. REV. 474 (2004).

[31] Roger Clarke, *Introduction to Dataveillance & Information Privacy & Definitions of terms* (2006), available at http://www.rogerclarke.com/DV/Intro.html (Last visited on November 1, 2010).

[32] Mathews Thomas, *supra* note 30.

[33] *Id.*

[34] *See* Sudhir Krishnaswamy, *Unique Identity Numbers: The Enabler of Policy Reform?*, January 2, 2010, available at http://casi.ssc.upenn.edu/iit/krishnaswamy (Last visited on November 21, 2010).

plagued the system – a problem which the mandate of the project promises to tackle. However, the exclusion of health information, religion and caste in the Bill may be attributed to the divisive and discriminatory character of such information. Unlike the Census whose primary purpose is to study demographic trends, such information with the CIDR could potentially be accessible to anyone, from government agencies to private individuals. The fact that these categories have been excluded is recognition that although *prima facie* the use of this information is severely restricted, the possibility of misuse, especially at the hands of the Government itself, is a very real possibility that needs to be avoided.

B. REGISTRARS UNDER THE BILL, AND MOUs SIGNED

As important as the kind of information to be collected, is who will collect this information. 'Registrar' has been defined as "any entity authorised or recognised by UIDAI for the purpose of enrolling the individuals".[35] The definition of Registrar includes government and public/private sector agencies which already have the infrastructure in place to interface with the public to provide specified services such as insurance companies, LPG marketing companies, banks,[36] National Coalition of Organisations for Security of Migrant Workers etc. The Registrar generally has a keen business and social interest in ensuring the authentic identity of the people availing their services.[37] Defined in §2(i),[38] the Enrolling Agencies, on the other hand, are the agents of the Registrar, which will directly interact with and enroll residents into the CIDR and will be monitored by the Registrars.

The question of who these registrars would be, finds no mention in the Bill itself. However, the UID has already appointed several Registrars by way of Memoranda of Understanding with various state governments and other institutions. The UIDAI's entering into MoUs with various state governments/ union territories and several banks, as per §23(3)(a)[39] of the Bill, is being hailed as a crucial step in the UIDAI's mission of providing UID numbers to the residents, in order to facilitate the availability of social welfare benefits to the poor residents. For instance, 'financial inclusion' is stated to be the the goal of the UID's first institutional partnership with Life Insurance Corporation (LIC) of India. Simply

---

[35] §2(o), the Bill.

[36] *See e.g.*, Bank of India, Canara Bank, Central Bank of India, Corporation Bank, Indian Bank, Indian Overseas Bank, Oriental Bank of Commerce, Punjab and Sind Bank, State Bank of India, United Bank of India etc.

[37] *See* Law Resource India, *Unique Identification Project*, January 6, 2010, available at http:/ /indialawyers.wordpress.com/category/uid-identity/ (Last visited on November 1, 2010).

[38] "Enrolling agency" means an agency appointed by the Authority or by the Registrars, as the case may be, for collecting information under this Act.

[39] The Authority may enter into Memorandum of Understanding or agreement, as the case may be, with Central Government or State Governments or Union Territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing,securing or processing of information or performing authentication.

put, such an MoU, by easy identification of customers, is meant to enhance LIC's efficiency in administration of the various social security schemes that are managed by it on behalf of the Government of India.[40] Similarly, the project of financial inclusion launched in Jharkhand with the Rural Development Department as the Registrar, envisages payment of wages to Mahatma Gandhi National Rural Employment Guarantee Act ('MGNREGA') workers at their doorsteps by using their biometric identity, thus curbing irregularities in wage payments to a great extent.[41] It could also serve as a remedy for the client-identity issue that banks are grappling with, which presents a potential win-win situation for both sides.

However the path of financial inclusion is fraught with hindrances – the fact that only 45% of the Indian population has bank accounts might act as a major roadblock in the aim of financial inclusivity –and it might be a daunting task for the UIDAI to help the 'marginalized' groups in such a scenario. Merely looking at the MoUs that have already been signed, it appears that having a UID number seems to be an important step in giving smooth and unhindered accessibility to services and products. In such a situation, it seems doubtful whether the voluntariness of enrollment for UID numbers will be maintained. In the future, these Registrars might, insist that their customers enroll on the UID to receive continued service.[42] Sunil Abraham, Director, Centre for Internet and Society, a Bangalore-based research organization is concerned that this would lead to an unwanted situation where lack of a UID number would result in denial of entitlements and benefits, and reccomends that such denial should be made an offence under the Bill.[43]

Very recently, UIDAI has entered into MoU with the Human Resource Development ('HRD') Ministry which aims at creating an electronic registry of all students to track student mobility, right from primary and elementary level through secondary and higher education, and also between the institutions.[44] Imprinting the UID number on the mark sheets, migration and merit certificates of students is aimed at serving myriad purposes like effective implementation of loan and scholarship schemes, mid-day meal scheme, and helping future employers by tracking fake degrees and duplicity of certificates. Most importantly, it can be linked to the Right to Education agenda, by easy identification of children from

---

[40] NetIndian News Network, *LIC Becomes First Institutional Partner in UID Project*, June 6, 2010, available at http://netindian.in/news/2010/06/09/0006786/lic-becomes-first-institutional-partner-uid-project (Last visited on November 1, 2010).

[41] Chandrabindu, *UID to Launch Financial Inclusion Pilot Projec*t, March 8, 2010, available at http://www.igovernment.in/site/uid-launch-financial-inclusion-pilot-project-38117 (Last visited November 1, 2010).

[42] *See* Usha Ramanathan, *supra* note 8.

[43] *See* Shafi Rahman, *Identity Crisis*, September 3, 2010, available at http://m.indiatoday.in/itwapsite/story?sid=111336&secid=134 (Last visited on January 10, 2011).

[44] Reporter, *HRD Ministry signs MOU with UIDAI,* THE ECONOMIC TIMES (Delhi) October 27, 2010.

downtrodden sections and facilitating their admission into neighbourhood schools. It goes as far as claiming to help arrest student drop-out rates by monitoring their performance and attendance records.[45] The MoU for delivering education-based programmes depicts that while initially they were entered into by the UIDAI with the objective of financial inclusion, MoUs are not just confined to that purpose. This widening ambit shows the eventual extension of this number to the everyday life of people, from their financial to education records.

IV. SUMMARY OF THE PROCESS OF THE AADHAR NUMBER SYSTEM

Before we move on to an analysis of the privacy implications of this project, it is important to scrutinize the process it will employ according to the provisions of the Bill.

A. STEP ONE: COLLECTION OF IDENTITY INFORMATION

The Bill provides for enrolling agencies to carry out collection of information in §2(i), whereas §2(o) defines the role of the Registrar as the entity authorized to enroll individuals under the Act. Both these definitions seem overlapping, but as described earlier, the system seems to be that enrolling agencies will act as agents of the Registrars, and enroll residents into the CIDR under their supervision. §3(1) of the Bill only adds to the confusion, by stating that every resident will provide the information *to the UIDAI* in order to obtain an 'aadhar' number (emphasis supplied). However, reading §2(i), §2(o) and §3(1) together, it is submitted that the intended meaning is that it is the enrolling agency and Registrars, and not the UIDAI directly, that will collect the information.

B. STEP TWO: VERIFICATION

This issue of whether there will be any verification of the information collected is left unclear in the Bill. Although, §3(2) states that verification will follow the receipt of the information, the term is not defined in the legislation. Even §2(d) which states that the 'aadhar' numbers and identity information will be submitted to the CIDR "*for verification"* appears to be referring to the process of authentication (emphasis supplied).

C. STEP THREE: ENROLLMENT IN THE CIDR

Subsequent to the collection and verification of identity information, it will be submitted to the CIDR. As explained in detail earlier, the Bill seems to focus on limiting the information that can be held with the CIDR by restricting it to

---

[45] Reporter, *UID Meets HRD: Now Electronic Registry of all Students*, The Indian Express, October 28, 2010, available at http://www.indianexpress.com/news/uid-meets-hrd-now-electronic-registry-of-all-students/703501/ (Last visited on November 12, 2010).

demographic and biometric information[46] and specifically excluding certain information under §9. Once again, in tandem with the trend of this legislation, §2(f) has an increased scope due to the words "other information related thereto" (emphasis supplied).

D. STEP FOUR: AUTHENTICATION

§2(d) describes this as a process by which the CIDR may verify the 'aadhar' number and identity information of the individual, by a simple check for compliance with the date available with it. §5(2) states that the UIDAI shall respond to an authentication query with "a positive or negative response or with any other appropriate response" without providing any substantive demographic information and biometric information (emphasis supplied). The format will go something like this – "Is Mr. X 18 years, Male, and living at 4, XYZ Road?" to which the UIDAI will respond in a Yes/No format.

E. STEP 5: UPDATION OF INFORMATION

§9 provides that 'aadhar' number holders will have to update their information as and when required, in order to maintain accuracy. As the duty is on them, it is expected that a quick, simple and accessible system of updating would be necessary.

In conclusion, the draft legislation leaves the all-important process of collection and verification of information shrouded in ambiguity. While the impression cast by §3(1)[47] is that the demographic and biometric data has to be submitted to the UIDAI, it is the enrolling agencies and registrars, drawing authority from §2(i) and §2(o) who are the de facto collectors of information. Delegation of such a critical responsibility raises grave issues of confidentiality. Although the Bill tackles the question of punishment in case of intentional misuse of information, it chooses to condone the situation of sheer negligence on the part of information collectors.[48] Another gaping flaw is the unanswered question of what procedure will be followed for verification of data before its incorporation in the CIDR database. Penalty for impersonation at the time of enrollment is prescribed in §34.[49] What the bill does make apparent is that the UID number will

---

[46] §2(f), the Bill.

[47] Every resident shall be entitled to obtain an aadhaar number on providing his demographic information and biometric information to the Authority in such manner as may be specified by regulations.

[48] §37, the Bill.

[49] Whoever impersonates or attempts to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information shall be punishable with imprisonment for a term which may extend to three years and with a fine which may extend to ten thousand rupees or with both.

be accepted as an identity proof, only after the authentication process,[50] and any authentication query will be responded to with a positive or negative answer, or any other response (which is not defined in the Bill), keeping in mind that no information is divulged.[51] For the management of the CIDR, including the maintenance and time-to-time updation, the UIDAI might rope in other entities in pursuance of §7[52] - once again eliciting confidentiality concerns. While it is only pragmatic to put the onus of informing the UIDAI regarding any change of information on the aadhar number holder, the Bill turns a blind eye to what will happen in case the UID number holder does not adhere to it.[53]

V. PRIVACY AND THE UID BILL: EXAMINING THE 'REAL', AND HYPOTHETICAL OUTCOMES OF THE PROJECT

'E-governance' does not just refer to new technologies in use by the government, but a system of governance that seems to suggest that the ills of inefficiency and corruption that plague the government can be corrected by the use of 'neutral' technology. One way of looking at this is reinventing social and political problems as technical ones, which can therefore, be fixed by technical solutions.[54] The UID project exemplifies the introduction of IT into governance,[55] and proposes the use of superior technology such as biometrics for the benefit of the poorest of India, among other things. Although technology is a great tool for progress, it is only as good, and as neutral as the manner of its use. In this section, we will examine how the Bill limits (or delimits) the usage of information for this project in the context of information privacy in India. We will compare the standards of the Bill to those in other legislations, to determine whether this legislation will be a step forward.

---

[50] §4(3), the Bill, stating that "An aadhaar number shall, subject to authentication, be accepted as proof of identity of the aadhaar number holder".

[51] §5, the Bill.

[52] The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

[53] §8, "The Authority may require the aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations so as to ensure continued accuracy of their information in the Central Identities Data Repository", the Bill.

[54] *See* Winner Langdon, Autonomous Technology, 2007 *cf.* Ravi Shukla, *Reimagining Citizenship: Debating India's Unique Identification System,* Economic and Political Weekly (Mumbai) January 9, 2010.

[55] *See* Samar Harlankar, *Play it again, Sam!,* The Hindustan Times, October 10, 2010. Recently, Sam Pitroda, Advisor to the Prime Minister of India on Public Information Infrastructure (PII) & Innovations recently announced the PII project to work in conjunction with the UID. While the short term plan is to connect 250,000 panchayats with fast broadband connections, the long term involves Geographical information systems (GIS), and massive fibre optic infrastructure. In this impassioned interview, he stated his vision for the new India - "UID tags every person, GIS every place and the applications we will build tags every government programme".

As far as the Indian Constitution goes, the right to privacy does not find explicit mention. The Courts, however, have asserted that the right to privacy may be read into the constitutional guarantee under Article 21.[56] In *R.Rajagopal v. State of Tamil Nadu*,[57] the Supreme Court held that the right to privacy was a fundamental right, enforceable against private persons as well. Just as the Apex Court has read in the right to privacy as a constitutional guarantee, it has also read in several restrictions. For the purposes of this article, we will analyze how these limitations provide the basis for justifying intrusions into privacy in the UID Bill as well as other legislations.

In *Mr. X v. Hospital Z*,[58] the Court held that in case of conflict between rights, the right which advanced 'public interest' or 'public morality' would be enforced by the Court. In *Gobind v. State of Madhya Pradesh*,[59] the Court held that an individual and "those things stamped with his personality" would be protected against official interference unless "a reasonable basis for intrusion exists". The same was upheld in the *PUCL v. Union of India*,[60] case, famously known as the 'wiretapping' case. While reasserting that privacy rights were part of the right to life and personal liberty, the Court held that such a right was not absolute and would remain *'subservient'* to the interest of the State (emphasis supplied).[61] While the Court may employ the rhetoric of "every man's house being his castle",[62] the right of the State to not only act in 'public interest' but also define the contours of what constitutes 'public interest', gives the State wide powers to intrude into anyone's castle. Further, although it is 'territorial' or 'spatial' understanding of a person's privacy which has been dealt with, recently, the courts seem to have adopted a more holistic view of the right to privacy existing 'in persons, not places'. In *Selvi v. State of Karnataka*,[63] the Court adopted a wider meaning of privacy, extending to "personal knowledge of a fact". It emphasized personal autonomy, holding that revealing a personal fact, was entirely in the domain of the individual's decision-making, which must be free from interference.

Yet in all these cases, be it phone tapping or medical tests on criminal suspects, the intrusion upon information was coercive – which makes it problematic

---

[56] Kharak Singh v. State of U.P., AIR 1963 SC 1295, ¶ 38 (*per* SUBBA RAO, J.).

[57] R.Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264, ¶ 10, 16 (*per* B.P. REDDY, J.).

[58] Mr.X v. Hospital Z, (1998) 8 SCC 296.

[59] Gobind v. State of Madhya Pradesh, AIR 1975 SC 1378, (*per* V.R.KRISHNA IYER,JJ.), ¶ 16

[60] *See* PUCL v. Union of India, (2003) 4 SCC 399.

[61] *Id.,* in observing that the right to privacy could "be denied only when an important countervailing interest is shown to be superior".

[62] Kharak Singh v. State of U.P., *supra* note 56, ¶ 19 (*per* AYYANGAR, J.).

[63] Selvi v. State of Karnataka, Criminal Appeal Nos. 54 of 2005, 55 of 2005, 56-57 of 2005. This case involved collection of medical data in criminal investigation, and it was held that involuntary medical tests on criminal suspects were a clear violation of the right to privacy.

to use them to interpret this Bill. In the UID system the provision of information will be 'voluntary' – the Bill does not explicitly mention this, but in all official documents the same has been emphasized.[64] However, the voluntariness only extends to the disclosure of information to enrolling agencies. Given that it has remained ambiguous to what uses such information will be put, and *who* will access it, it is yet to be seen whether such decisions will incorporate the consent of the individual. No such impression has been made till date. While this voluntary nature itself may be questioned, even assuming this to be correct, it, by no means, suggests that no privacy intrusion is possible under the Bill. For understanding the same, we now examine data protection laws in foreign jurisdictions, where 'information privacy' is a separate and nuanced field of law.

The very controversial ID card project in the U.K.[65] was subject to the principles laid down in the Data Protection Act, 1998. The first two principles state the general rule that "Personal data shall be processed fairly and lawfully and in accordance with certain prescribed conditions", while the second states that "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".[66] This statutory purpose is to include not only what information is used but also to whom it potentially may be available. Whether or not cardholders have this knowledge of who will have access to this information will decide its legality and is known as the 'fairness test'. The Apex Court in India too has devised several similar 'tests of reasonableness' for legislative intrusions/ executive orders/judicial orders. Yet these have remained broad principles for judicial interpretation, and nowhere have the courts given specific guidelines for cases of data protection.

While the U.K. has a comprehensive data protection law for personal data in general, in the U.S. there are multiple legislations, which tackle privacy issues involved in different sectors such as Privacy Act, 1974, Computer Matching and Privacy Act, Video Privacy Protection Act etc.[67] The Privacy Act, 1974 serves to protect personal data and individual rights over information contained in federal

---

[64] *See* Graham Greenleaf, *India's National ID System: Danger Grows in a Privacy Vacuum,* July 13, 2010, available at http://www2.austlii.edu.au/~graham/publications/2010/India_ID_system0710.pdf (Last visited on January 7, 2011).

[65] The National Identity Cards Act of the U.K. was passed in March 2006, but has been repealed in May 2010. Its stated purpose was to tackle illegal immigration and identity theft, but received widespread dissent due to high costs and infringement of civil liberties. The Cards held biometric information in an encrypted chip. *See* BBC News, *Identity cards scheme will be axed 'within 100 days'*, May 27, 2010, available at http://news.bbc.co.uk/2/hi/8707355.stm (Last visited on November 21, 2010).

[66] Principle 1, 2, Schedule 1: The Data Protection Principles, UK Data Protection Act, 1988.

[67] Jean Slemmons Stratford & Juri Stratford, *Data Protection and Privacy in the United States and Europe*, Paper presented at the IASSIST Conference, May 21, 1998, at Yale University, available at http://www.iassistdata.org/downloads/iqvol223stratford.pdf (Last visited on November 21, 2010).

databases.[68] Similar to the Data Protection Act of the U.K., it emphasizes that information may only be disclosed with the individual's consent and that the purposes must be announced in advance.

In the backdrop of these foreign laws on data protection, it is plain to see that information privacy involves a more meaningful understanding of consent, than the one projected by the UIDAI. It mandates that individuals must be informed in advance on how the data they provide is being utilized and to what purposes. From this perspective, we can begin our analysis on the issues of privacy involved in the Bill.

A. AUTHENTICATION

As explained earlier, the Bill vests the power in the UIDAI to authenticate the aadhar number with the information in the CIDR by way of Yes/ No answers.[69] The Bill clarifies that the UIDAI will have the power to develop all policy, procedure and systems for the implementation of aadhar numbers and in particular, with the process of authentication under the Act.[70] The powers of the UIDAI may include "performing authentication of 'aadhar' numbers".[71] The Bill also reiterates that the UIDAI will have power to make any rules regarding authentication.[72] Details of authentication requests to the UIDAI or any of the Registrars must be recorded along with responses and provided to the aadhar number holder on request. §33 makes a provision for when information may be disclosed pursuant to a Court/Executive order whereas penalties for fraudulent requests for authentications are covered under §40.

It is amply clear that while the above provisions cover some aspects of authentication, several gaping holes remain. The first question that requires clarity is who can ask for authentication. In light of the existing legal framework of data protection laws in the U.K and U.S., the question of to whom information may be made available is of paramount importance. Both laws mandate that this information must be made available to the individual prior to the collection of information. It may be argued that given that the purpose of the Bill is directed towards "*accessing public benefits and services"* (empasis supplied),[73] this policy guideline is sufficient in order to determine the kinds of persons/institutions/ companies that may request for authentication. However, the UID project has been purported to play a role in national security from its very inception. This

---

[68] S.Bhushan, *The UID Project: The 1984 Of Our Times*, available at http://ssrn.com/abstract=1598596 (Last visited on November 21, 2010).

[69] §5, the Bill.

[70] §23(1), the Bill.

[71] §23(1)(e), the Bill.

[72] §54(2)(e), the Bill.

[73] Statement of Objects and Reasons, the Bill.

purpose itself is plagued with concerns of tracking and profiling of citizens. While this will be described in detail subsequently, it suffices to say, that the purposes of this project are far from limited, even from a look at official documents. Further, given the sensitive nature of demographic and biometric information, it appears imperative that such a legislation list which kind of persons/institutions/ corporations can make requests for authentication.

B. CONVERGENCE, TRACKING AND PROFILING OF INDIVIDUALS

As it stands today, information about individuals that are given to companies, banks, governmental agencies and departments are held in 'silos', discrete towers which hold specific information provided for a specific purpose/ service (Driving License, Voter ID Card, Ration Card).[74] In the alternative, this data could be organized into a central database. However, there is a strong argument that correlated data provided to a single institution must be minimized, and at least be provided for in different databases, where each different institution is responsible for protection of such data as per law. Certain legal academics like Usha Ramanathan opine that the UID will serve to link these discrete silos, a process known as 'convergence', and therefore unleash the capability to profile an individual on the basis of personal data.[75] Convergence of information allows third parties, including private companies to utilize such information to harass a person. A common example is the way private companies obtain access of personal details of individuals and pursue aggressive marketing strategies through phone and email in ways that intrude upon their privacy. The official response to these claims has been that such convergence is already possible given the existence of mobile numbers, PAN card numbers, passport numbers etc. which can all converge personal data about an individual and be used by agencies.[76] Further, it is argued that given that information of race, religion, caste, tribe, ethnicity is excluded by the bill, profiling is not possible. Even if we accept that such convergence is not facilitated by the UID in particular, it is clear that the UID may provide a common denominator on the basis of which agencies may connect the data they have. In fact, one of the selling points of the project has been that the aadhar numbers will enable de-duplication of other databases as well such as the National Population Register for example. This necessarily involves convergence with duplicate-infested erroneous data.[77] De-duplication is dependent on the reliability of one-to-one matching, and it is yet to be seen whether this will be efficient. However, what is clear is that convergence of data is an integral part of the UID project, which many see as a tool which may be put to intrusive purposes.

---

[74] *See* Usha Ramanathan, *supra* note 8.

[75] *Id.*

[76] R.S. Sharma, *Identity and the UIDAI: A Response*, Economic and Political Weekly (Mumbai) August 28, 2010.

[77] Ruchi Gupta, *supra* note 4.

This aadhar number is unique in that it corresponds to biometrics which may be used by an individual throughout his/her life for all major transactions. This itself has led to concerns of it enabling tracking of individuals by the Government. Let us examine this claim in light of the debate which ensued in the UK with regard to the draft legislation of the Identity Cards Act, 2006. It was feared that every time an organization has checked an individual's card, or requested for authentication such a record would create an 'audit trail' which could be accessed by a court or executive order, enabling the government to essentially track an individual's actions.[78] The Indian Bill makes no such explicit reference; however, the fact that such a record will be maintained may be inferred from §33, which states that the Authority may be required to share "identity information" along with "details of authentication" the latter referring to all requests for authentication of identity which have been received by the UIDAI (emphasis supplied). This record may be compared to that of an 'audit trail', as such records will reveal much about the 'aadhar' number holder's daily activities from accessing the PDS, to bank records, travel records, and even education records as per the most recent MoU signed with the HRD Ministry. It is obvious that such information is sensitive, and may be misused for tracking an individual's actions. In light of the same, the Bill restricts the disclosure of this record, only allowing it when there is a specific order of a competent court for the same. It does not involve the consent of the individual; however, given the capability of misuse of this provision it has been urged that the concerned person should at least be given the right to be notified of such disclosure in advance, or generally be given an opportunity to resist the same.

VI. NATIONAL SECURITY RATIONALE OF THE UID

Right from the initial government press releases in November 2008, the national security rationale of the UID project was apparent: "better targeting of government's development schemes, regulatory purposes, national security purposes, banking and financial sector activities".[79] In fact, if we delve into the origins of the UID project, we find that national security actually formed the initial justification for the same. It was the Kargil Review Committee Report, published in 2000 under the NDA Government, which noted the need to provide ID cards to the population, especially those in border districts.[80] In 2001, the Group of Ministers submitted its report titled 'Reforming the National Security System' which proposed a compulsory Multi-purpose National Identity Card ('MNIC') to aid the creation of the 'National Population Register' ('NPR') of citizens' and tackle illegal

---

[78] *See* The LSE, *The Identity Project: An assessment of the UK Identity Cards Bill and its implications*, June 27, 2005, available at http://is2.lse.ac.uk/IDcard/identityreport.pdf; *see also* Jennifer Morris, *Big Success or "Big Brother?": Great Britain's National Identification Scheme Before the European Court of Human Rights* 36 GA. J. INT'L & COMP. L. 465 443 (2007-08).

[79] *See* R.Ramakumar, *High Cost-High Risk*, THE FRONTLINE (New Delhi) Aug. 01-14, 2009.

[80] *Id.*, *see also* R.Ramakumar, *What the UID conceals*, THE HINDU (New Delhi) October 21, 2010.

migration. To facilitate this, the preparation of this national register was clubbed with the Census. To this end, several privacy clauses in the Citizenship Act of 1958 were diluted by way of the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003,[81] and the post of Director of Citizen Registration (to also function as Director of Census) was created. Onus for registration in the NPR was put on the citizens, and the information required for the register was under 15 heads, including name, sex, date of birth, parents' details, present and permanent address, marital status and "if ever married, name of spouse". When the UPA Government came into power, this MNIC project was replaced by the Bill. Finally, UIDAI's formal establishment itself was announced as a response to the 2008 Mumbai terror attacks in January 2009 by Home Minister Mr. P. Chidambaram.[82]

Although the UIDAI has remained silent, and even evaded any responsibility regarding the use of the project for security purposes,[83] its history shows that it is very much a part of the new national security plan of the Government of India. Its connection with the NPR has also been made explicit by both the Census Commision[84] and Chairman Nilekani who is quoted as stating that the UIDAI will act as "the back- office of the NPR by 'de-duplicating' the collected data to generate the UID".[85] Simultaneously, the Central Government has announced its plan to create a National Intelligence Grid ('NATGRID') which connects the databases of 11 agencies, such as the Investigation Bureau ('IB'), Research and Analysis Wing ('RAW'), Central Bureau of Investigation ('CBI'), Central Board of Direct Taxes, Central Board of Excise and Customs, although the

---

[81] Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003,notified in the Government of India Gazette Vide GSR No. 937(E) dated:- 10 December, 2003, introduced several provisions such as "§14A (1) The Central Government may compulsorily register every citizen of India and issue national identity card to him.

(2) The Central Government may maintain a National Register of Indian Citizens and for that purpose establish a National Registration Authority.

(3) On and from the date of commencement of the Citizenship (Amendment) Act, 2003, the Registrar General, India, appointed under sub-section (1) of §3 of the Registration of Births and Deaths Act, 1969 shall act as the National Registration Authority and he shall function as the Registrar General of Citizen Registration.

(4) The Central Government may appoint such other officers and staff as may be required to assist the Registrar General of Citizen Registration in discharging his functions and responsibilities.

(5) The procedure to be followed in compulsory registration of the citizens of India shall be such as may be prescribed."

[82] R.Ramakumar, *supra* note 79.

[83] *See* R.S. Sharma, *supra* note 76.

[84] NPR is linked to the unique identification number (UID) project. We will provide the data to the UID authority. It will scan the biometrics and inform us if there are double or triple biometric signs. We will physically check and inform the authority which data should be accepted.

[85] Praful Bidwai, *supra* note 9.

project still awaits approval of the Cabinet Committee on Security.[86] Under the NATGRID scheme, telecommunication and internet service providers will compulsorily have to link their databases as well, along with rail and air travel, phone calls, bank accounts, passport and visa records, PAN cards.[87] The NATGRID has alarmed many with its aggressive, and indeed all pervasive system of integration of databases and its resultant capability to fully profile individuals. Its link to the UIDAI has been suspected by many, who argue that the UID number will be the essential link between databases that will facilitate the process.[88] However, no official statement regarding this link has been made.[89]

As we discussed earlier, national security finds no mention in the Statement of Objects of the Bill. However, the Statement of Objects and Reasons remain a external aid to interpretation of a Statute[90] and §33(b) of the Bill widens the objectives that the Act seeks to achieve. It allows for disclosure of information possessed in the CIDR if it is made "in the interests of national security pursuance of a direction to that effect issued by an officer not below the rank of Joint Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge". Unlike §33(a) which allows for disclosure of information pursuant to the order of a competent court, this provision not only bestows the same power on the executive, but recognizes that a justification for doing so is imperative, making the purpose of national security explicit.

It is important to note that under §33(a) both 'identity information' and 'details of authentication' may be disclosed pursuant to a court order. The latter category, as explained earlier, would be a record for all times that authentication of that 'aadhar' number has been requested, including by whom, when and where. Interestingly, §33(b) which allows for disclosure by executive order in pursuance of national security only allows disclosure of 'identity information' and not 'details of authentication'. As explained earlier, details of authentication would give the government the capability to track an individual's actions by way of travel records, education records, back records etc. If such information has been excluded from the reach of the government, it may be seen as a deliberate measure to protect privacy.

---

[86] Live Mint, *Home Min Starts Consultation for NATGRID With Stakeholders*, January 2, 2010, available at http://www.livemint.com/2010/01/03152443/Home-Min-starts-consultation-f.html (Last visited November 21, 2010); *see also* Sahil Makkar, Live Mint, *CCS approves NATGRID plan*, May 12, 2010, available at http://www.livemint.com/2010/05/12221213/CCS-approves-Natgrid-plan.html (Last visited on November 21, 2010).

[87] *Id.; see also Govt Plans NATGRID to Tackle Terror*, REDIFF NEWS, available at http://news.rediff.com/report/2010/feb/06/natgrid-will-track-all-your-spending.htm (Last visited on November 21, 2010).

[88] *See* Usha Ramanathan, *supra* note 8; Ruchi Gupta, *supra* note 4; Praful Bidwai, *supra* note 9.

[89] *See* R.S. Sharma, *supra* note 76.

[90] GP SINGH, PRINCIPLES OF STATUTORY INTERPRETATION, 238.

VII. PRIVACY STANDARD IN OTHER LEGISLATIONS

A legislation which also directly affects the privacy of citizens in the name of national security is the Indian Telegraph Act, 1885. It regulates phone tapping by §5(2), which states that on the occurrence of either public emergency or in the interest of public safety, the Government may direct the interception, or detainment or disclosure of any messages transmitted or received by any telegraph "if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence". Other sections provide for the government formulating "precautions to be taken to for preventing the improper interception or disclosure of messages"; however, till date, no such rules have been formulated. In the writ petition filed in the Apex Court, People's Union for Civil Liberties challenged the constitutional validity of §5(2) on the ground that it violated the right to freedom of speech and expression and to life and personal liberty.[91] The Supreme Court recognized that phone tapping was a "serious invasion of an individual's privacy",[92] and in view of the major technological advances, the privacy of individuals in their own homes was under threat. The Court laid down several guidelines to be adhered to before sanctioning the tapping of any telecommunication. As in the Bill, the justification for such interference was built on the premise of public safety, along with public emergency. The term public emergency was defined by the Court as the "prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action", and public safety as "the state or condition of freedom from danger or risk for the people at large". The Court held that the fulfillment of these conditions was the sine qua non for any government order to tap phones.

Far more intrusive in a sense, is the amendment to §69 of the Information Technology (Amendment) Act, 2008. It states that:

"(1) Where the Central Government or a State Government or any of its officer specially authorised by the Central government or the state government, as the case may be, in this behalf, may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource."

---

[91] PUCL v. Union of India, *supra* note 60.

[92] *Id*. at ¶1 (*per* KULDIP NAYAR, J.).

This section does away with the reference to public emergency or public safety present in the Telegraph Act. Unlike the earlier IT Act of 2000, it widens the scope of government intrusion from only decryption of messages to interception and monitoring, which were not mentioned earlier.

In terms of when and by whom personal information/communication may be disclosed, the standards in these various legislations may be compared. The Bill in §33(b) allows for disclosure of information to the Central Government alone, unlike the Telegraph Act which vests this power with the state government as well. It also allows this power to any officer of the Central Government as opposed to the Bill which specifies that the officer must at least be the rank of Joint Secretary or its equivalent. The IT Act also gives a sweeping power to any officer of the state or Central government. However, important to note is that while both the Telegraph Act and the IT Act mandate that the Government official must record, in writing their reasons in detail, the Bill makes no such requirement.

Furthermore, the IT Act and the Telegraph Act both require satisfaction that such an action is 'necessary' or 'expedient' in the interest of sovereignty, integrity of India, defence of India, security of the State, friendly relations with foreign States, public order etc. Unlike the gamut of circumstances provided, the Bill gives merely one, relatively ambiguous criteria of 'national security'. This combined with no requirement to make any formal record of justification, gives the Government significant leeway to order for such disclosure.

Insofar as the Bill restricts this power to senior officials of the Central Government alone, this is a welcome measure, but by no means does this provision adequately address concerns for misuse. Finally, it is evident that there doesn't appear to be a uniform, or even predictable standard of privacy applied in to such provisions in various legislations.

VIII. CONCLUSION

The media in India is abuzz with talk of unique identification, of connecting panchayats through broadband connectivity, of geographical information systems and fibre optic infrastructure. Yet few of us are adequately informed about what such systems will translate to in reality. Sam Pitroda, advisor to the Prime Minister on Public Information Infrastructure, recently shared his vision for the new India: every person 'tagged' by the UID, every place mapped by GIS, and applications that could tag government programmes. It seems that we are reaching out to technology, previously restricted for the use of the wealthy,address issues of poverty, and corruption. This is 'revolutionary' to the extent that it signals a new method of governance, but beyond that, the assumption that technology itself eliminates error and human subjectivity is extremely problematic. Through this article, we have maintained that technology itself is fallible and open to grave misuse, and therefore its use must be carefully regulated. This has formed one of the bases of critique of the UID project. Recent controversies surrounding acts labelled as 'seditious' have brought out a panic among citizens

about being targeted by the State for political or other beliefs. Other incidents of phone tapping which revealed murky secrets of the powerful in India created awareness that perhaps no one, not even the powerful, can choose what information they keep private. In this era of surveillance of all kinds, there is increased suspicion about bringing a person's personal information into the public domain, as it gives the holder of such information immense power over you. While this may be perceived as unwarranted paranoia, information privacy is a reality that is being acknowledged and protected world over. Thus, the National Identification Authority of India Bill has been introduced at a time where issues of privacy have recently taken the forefront in public debate in India

Unlike similar projects in other jurisdictions such as the U.K. and U.S., which take the justification of national security the UID has built its mandate on increasing access to social welfare program which has gained easy acceptance among the public, given the problems of fraud and corruption that plague existing identification mechanisms. We did not examine whether or not access to social welfare benefits would be enabled by this scheme. From confusions regarding who will collect the information, to silence about who will be permitted to make requests for authentication, it seems as though this legislation has intentionally given the UIDAI ample scope to decide as it goes along. The fact that the funds have been sanctioned, and first UID numbers have already been allotted long before this bill is passed in parliament is testament to the fact that this project is definitely not waiting for legislative sanction or regulation.

We infer that despite the UIDAI's continual restatement of the restricted use of such data for mere authentication in welfare programs, the expicit prohibition in §9 is recognition that possibility of misuse is a real possibility that must be avoided.

A look into the various MoU's signed for Registrars under the Act reveals the pervasive role that this number will have on our everyday lives. It also leads us to challenge the supposed voluntary nature of such a program, as it seems that several essential/beneficial services will be made available only by obtaining the UID number. If consent of individuals forms the basis of collection of such personal information under the UID project, then attaching a penalty, whether legal or financial, for not having a UID number is a possibility that must be avoided.

In this article we used the Bill as the primary indicator of the intrusions of privacy that will be permissible under this project, in order to analyze the affect of this project on privacy of citizens. What is most disturbing is the silence in the Bill regarding *who* will be enabled to request information under this law, even though such information is recognized as necessary in most privacy legislations abroad. Given that demographic and biometric data is inherently sensitive, it is important that the Bill in some way restrict which kind of persons/institutions/ companies can make requests to the UIDAI. Other concerns common to anti data consolidation programs across the world, is that of convergence in a central

database which could unleash threats of profiling diverse information about an individual. The UIDAI has rightly pointed out that convergence of data in our time is not particular to the UID. However, whether it is the National Population Register or the National Information Grid, they all seem to see the UID as the 'key' or common denominator on the basis of which agencies can connect data and identify it to a particular person. Convergence and tracking (which would be enabled by details of authentication with the UIDAI) are concerns which strike at the root of fear among citizens of an all pervasive surveillance regime.

The backdrop of national security in which this project was initially envisioned, is surprising given that the publicity surrounding the project has remained singularly focussed on access to social welfare benefits. It remains unclear how the CIDR database will supplement other data consolidation programs aimed at national security such as the NPR and NATGRID. The criticism to the UID link with such programs is based in a deep rooted skepticism that India is moving more and more towards a 'police state'.

Even with its several ambiguities, the Bill has been a welcome measure in some senses. In a country where discussions on privacy are severely restricted, the widespread debate started on the UID project have revealed a new side to the story, of intrusions of the privacy of the individual by the State. While the Courts have always accepted 'public interest', and 'national security' as reasonable restrictions on privacy rights, the right of the State to not only act in 'public interest' but also define the contours of what constitutes 'public interest', gives the State wide powers to intrude into anyones privacy. Hence, the debate surrounding this project has forced civil society to question the understanding of these terms themselves. The Bill is legal recognition of the harms possible from misuse of sensitive data, as evidenced by the prohibition on certain criteria of information. Subtle omissions, such as not allowing disclosure of *'details of authentication'* except by the order of competent Court, not even in the interest of national security, reveal recognition of the very eminent possibility of misuse of a centralized database.

The terms 'National security', 'the security of the nation', 'the interests of the nation', and 'public order' are the different terms used in legislations such as the IT Act and the Telegraph Act to justify intrusions into privacy. All these terms seem suitably overlapping, and suitably vague. Further, we conclude that no uniform legal standard exists for intrusions into privacy among these legislations. In fact, in recognition of the deficiencies surrounding the law on privacy, the Government has proposed to enact its first law to safeguard privacy. A panel of senior officials have been been appointed to prepare a blueprint for the same, and this proactive measure seems directly in response to concerns emanating from increased data collection by the Government for the UID and proposed NATGRID projects.

Cynicism and suspicion surrounding this project mustn't be viewed as an unhealthy development, as it reflects a new awareness among people towards

privacy and State surveillance. Questioning of this nature is integral to ensuring participation of people in decisions regarding governance. It is hoped that the final legislation will remedy the gaps in procedure and include privacy safeguards, so that this 'move forward' is one which rests on the meaningful.