

University of New South Wales
University of New South Wales Faculty of Law Research Series
2011

Year 2011

Paper 46

India's National ID System: Danger Grows in
a Privacy Vacuum

Graham Greenleaf*

*University of New South Wales, g.greenleaf@unsw.edu.au

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps11/art46>

Copyright ©2011 by the author.

India's National ID System: Danger Grows in a Privacy Vacuum

Graham Greenleaf

Abstract

India is juggling demands and proposals for at least three national data surveillance projects of vast scope. This article focuses on the unique identification (UID) number (called the Aadaahar), which it is proposed will be allocated to India's 1.2 billion people, with 600M UIDs to be allocated by 2015. The draft National Identification Authority of India Bill 2010, drawn up by the Unique Identification Authority of India (UIDAI) as legislation to formally create the Authority which will administer the UID, contains few protections for privacy or other liberties. They are needed because there is otherwise a privacy vacuum in Indian law.

The draft Bill leaves most of the details of the demographic and biometric information which will be required to be included Regulations, and imposes no controls on which organisations can require UIDs, or what they can do with them. This article focuses on the planning documents for the UID, and the Bill, to argue that India may be building an identification system that puts peoples' liberties at risk, and does so in a way which will be largely out of control of democratic or judicial restraints on such a powerful use of information technology. This article argues that the current operation of the aadhaar, and the draft Bill are deficient in that they lack at least the following protective provisions:

(i) Outsourcing of the operation of the CIDR should be by regulations identifying the outsourcing provider, and thus disallowable. Any movement of CIDR data outside India should also be by regulations. (ii) The Central Information Commission, or a similarly independent tribunal, should be empowered to adjudicate all disputes between the Authority and individuals. (iii) Individuals should be able to obtain compensation and injunctions for any breaches of their rights. (iv) The biometric and demographic information which can be collected by the Authority

should be defined in the Bill, and collection of other personal data prohibited. New legislation, and thus positive Parliamentary approval, should be required for any expansion. (v) The Bill should clarify whether obtaining a UID is compulsory or voluntary, and whether services may be denied to people because they do not have one. (vi) If the UID is voluntary, any special measures in relation to marginalised groups should also involve special steps to ensure that voluntariness is respected. (vii) Incentives given to any persons involved in the enrolment process should be designed to ensure that voluntariness is respected. (viii) UID holders should not be required to update their identity details unless this is necessary for the integrity of their UID and authentication. A continuously updated population register is not necessary for an ID number. (ix) The legislation should specify with which other agencies, and in relation to which benefits, the CIDR data can be shared, and any future changes should also be by legislation. (x) It should be prohibited for anyone to require a UID holder to obtain their CIDR data. (xi) It should be prohibited for any other databases to record the UID number.

Amendments such as these would not necessarily make the UID safe for India's 1.2 billion people, but they would reduce the risks of abuse. As India's economy and society become increasingly similar to those of other successful capitalist economies, the Indian government will increasingly need to adopt a full data protection law, as is the case throughout Europe and in an increasing number of countries in the Asia-Pacific. It has often been the case that the introduction of a new data surveillance system such as an ID card or a data matching system has shown the need – and provided the political trade-off – for the introduction of a full data protection law.

Note: The Bill that is analysed in this article, which was written in July 2010, differs in some respects from the Bill introduced into the Indian legislature, and which is due for debate in November/December 2011.

India's national ID system: Danger grows in a privacy vacuum

[Graham Greenleaf](#), Professor of Law & Information Systems, University of New South Wales*

19 July 2010

Published in (2010) Vol 26 No 5 [Computer Law & Security Review](#) 479-491

Abstract: India is juggling demands and proposals for at least three national data surveillance projects of vast scope. This article focuses on the unique identification (UID) number (called the Aadaahar), which it is proposed will be allocated to India's 1.2 billion people, with 600M UIDs to be allocated by 2015. The draft *National Identification Authority of India Bill 2010*, drawn up by the Unique Identification Authority of India (UIDAI) as legislation to formally create the Authority which will administer the UID, contains few protections for privacy or other liberties. They are needed because there is otherwise a privacy vacuum in Indian law.

The draft Bill leaves most of the details of the demographic and biometric information which will be required to be included Regulations, and imposes no controls on which organisations can require UIDs, or what they can do with them. This article focuses on the planning documents for the UID, and the Bill, to argue that India may be building an identification system that puts peoples' liberties at risk, and does so in a way which will be largely out of control of democratic or judicial restraints on such a powerful use of information technology.

1. Introduction.....	3
1.1 Enter the Aadhaar.....	3
1.2 Analysing ID systems.....	3
1.3 India's data protection vacuum.....	4
2 India's converging data surveillance context	5
2.1 National Population Register (NPR).....	6
2.2 National Intelligence Grid (NatGrid).....	7
2.3 The Multipurpose National Identity Card (MNIC).....	7
3 The Authority: Establishing the ID number system	8
3.1 The UIDAI or 'National Identification Authority of India'.....	8
3.2 Outsourcing India's identity repository?.....	8
4 The unique ID number (aadhaar)	8
4.1 Randomness as privacy and freedom.....	9
4.2 From birth to 'inoperative'.....	9
4.3 Between pseudo-voluntary and compulsory.....	9
4.4 Entitlement without rights.....	10
4.5 'Special measures': Identifying tribals, itinerants and the disabled	10
5 Biometric and demographic data to be collected.....	11

* Research for this article was conducted as part of an Australian Research Council 'Discovery' project, 'Interpreting Privacy Principles' <<http://www.cyberlawcentre.org/ipp/>>. Some work toward this article was published in *Privacy Laws & Business International Newsletter*, Issues 103, 105 and 106. Thanks to Jill Matthews for editing, and for helpful comments an anonymous reviewer, Ruchi Gupta and Usha Ramanathan. This article was also part of a submission by the author to the Unique Identification Authority of India (UIDAI).

5.1	<i>Biometric information</i>	11
5.2	<i>Demographic information</i>	12
6	The number allocation process	13
6.1	<i>Registrars, enrollers and introducers</i>	13
6.2	<i>Registration process</i>	13
6.3	<i>Cash incentives for enrolment</i>	13
7	Uses of UIDs and CIDR data by UADAI	14
7.1	<i>Authentication</i>	14
7.2	<i>An updated population register</i>	14
7.3	<i>Privacy protections concerning CIDR</i>	15
7.4	<i>Exceptions to the prohibition on disclosures from CIDR</i>	15
7.5	<i>Criminal penalties and compensation for abuses</i>	16
8	Use of the UID number and ID tokens by others	17
8.1	<i>Let a thousand ID cards bloom</i>	17
8.2	<i>Inclusion of the UID in other databases</i>	17
8.3	<i>Repeated requirements to document identity?</i>	18
9	Conclusions and recommendations	18
9.1	<i>'Designed to be out of control?'</i>	19
9.2	<i>Fait accompli?: Awareness, consultation and dissent</i>	19
9.3	<i>What is lacking in the Bill's privacy protections?</i>	20
	References	21

1. Introduction

1.1 Enter the Aadhaar

India is juggling demands and proposals for at least three national data surveillance projects of vast scope, and is now taking its first steps toward a universal identification system. The first project underway, and the main focus of this article, is the Unique Identification Number, development of which has commenced under the Unique Identification Authority of India¹. The UIDAI, charged with allocating unique ID numbers to the approximately 1.2 billion residents of India, was established in February 2009. It plans to issue its first ID number 'between August 2010 to February 2011' and by 2015 plans to issue 600 million 'UIDs' through various public and private sector 'registrar' agencies across the country. Some claim this will be world's largest IT project. The UIDAI's system is not in itself supposed to result in a national ID card, just a unique universal number, and a register of biometric and demographic information, on all residents (not only citizens) of India.

The UID system is currently developing without a legislative basis, and in the absence of any significant data protection laws in India. However, on 30 June 2010 the UIDAI released a draft *National Identification Authority of India Bill 2010* (the Bill², to which section references in this article refer, unless specified otherwise), requesting public comment within two weeks³. The draft legislation is incomplete in that large areas of its substantive content are to be included in regulations and rules, which are not included with the draft. This can be a common tactic of governments who wish to keep the bad news hidden until later regulations reveal them, or it can be represent the difficulty of drafting complex administrative details as early as broad policy directions. Important matters of policy should go in legislation, not regulations. That is a deficiency here, and it makes analysis at this stage incomplete.

In April 2010 the UID project was renamed 'Aadhaar', which means 'foundation', and a new logo based on a sun and a fingerprint was unveiled. It is claimed that 'aadhaar' communicates 'across all regional languages' in India (*Economic Times*, 2010). The Bill refers to the 'aadhaar number' and 'aadhaar number holder' (s2) but this article will stick to 'UID' and 'UID holder', as those are the terms used in most discussion to date.

This article is a critical analysis of the UID project and its implications for privacy in India, based on the draft Bill, planning documents available from UIDAI, and press reports. It aims to provide a basis for further analysis and for comparison with subsequent iterations of the scheme as it develops, and concludes for improvements to the draft Bill.

1.2 Analysing ID systems

'Identification systems have become a key mode of governance in the early years of the twenty-first century' claim Lyon and Bennett (2008:3) in the opening words of the most extensive text on this subject (Bennett and Lyon, 2008). Torpey (2000) showed that passports represented a new dimension of modernisation, the state's monopolisation of the regulation of movement. Amore (2008) and other authors claim that other identifiers and tokens, and

¹ UIDAI website <<http://www.uidai.gov.in/>>

² The draft Bill is available under 'Legislation and Guidelines' at <<http://www.uidai.gov.in/>>

³ The UIDAI has not made submissions public on its website. The only other known submission is by Gupta (2010b).

the information systems within which they work, go much further than regulating movement and increasingly regulate identification and identity *per se*.

The analysis of any national identification scheme requires attention to all aspects that contribute to it, including (at least) the number, the biometrics and other identification data collected, the underlying computer system, the tokens (cards or others) carrying the number, the uses to which it is permissible to put the number and the tokens, and the parties who are allowed to participate in any aspect of the system's operation. We must also ask what legal or other guarantees are there that these matters will not change over time (usually called 'function creep'). To focus only on the elements emphasised by the scheme's proponents is likely to lead to privacy and other dangers being overlooked. Focusing on one element of a system, such as card or a number, is a mistake. This topic is often mis-labeled 'ID cards'. 'But the card is only the visible evidence of complex and more latent systems of identification' insist Lyon and Bennett (2008: 3), and another author has phrased a similar caution as 'Contemporary modes of identification ... operate primarily via the screen and not via the card' (Amoore, 2008: 23).

This analysis is primarily from the perspective of legal regulation of surveillance systems. Here, as with other legislation governing many complex personal information systems, 'the devil lies in the details', and the details are usually technical and superficially boring. The meaning and operation of the legislation is not at all apparent on its face, many provisions appear to give protection that is then taken away by less obvious provisions, and much of the danger still lies in as-yet-unknown regulations or (worse) decisions by the system operator that are not even subject to Parliamentary scrutiny. As we will see, India's ID scheme and its enabling legislation is subject to all these 'features'. They are not bugs, as studies of proposed ID schemes in many other countries, including those by the author concerning Hong Kong (Greenleaf, 2008) and Australia (Greenleaf, 1987, , 2007, 2008a) have shown. The systematic and comparative study of ID systems is as yet limited, the most detailed study being the papers collected by Bennett and Lyon (2008), covering a dozen jurisdictions.

Many perspectives other than a legal analysis are needed to do justice to a development as complex as India's ID systems, including analyses of whether they will deliver better social incomes to disadvantaged people as claimed; of the role played by the private sector in influencing or determining the technical directions of the systems; of the historical and cultural factors leading to acceptance or rejection of different systems; and of the constitutional implications of the changes to the relationships between citizen and state. But all of these perspectives need to be informed by detailed knowledge of the legal framework within which the systems will operate.

1.3 India's data protection vacuum

India has no effective protection of information privacy, either through legislation or court decisions (Greenleaf, 2010 provides a 40 page summary). The *Information Technology (Amendment) Act 2008* contains a few fragments of data protection rights, but the only significant one is not yet in force (Greenleaf, 2009). The Constitution of India provides that 'No person shall be deprived of his life or personal liberty except according to procedure established by law' (Article 21). The Supreme Court has interpreted this provision to include the protection of privacy since *Kharak Singh v. The State of U. P.* [1962] INSC 377; 1963 AIR 1295 1964 SCR (1) 332. This was advanced beyond issues of search and surveillance by the Delhi High Court's decision to strike down provisions criminalising homosexual sexual conduct on grounds of invasion of privacy (*Naz Foundation v Government of NCT of Delhi* WP(C) No.7455/2001 (2 July 2009). The broadest statement of the Delhi High Court's approach is where, following its review of Indian case law to date on protection of privacy, it states "The right to privacy thus

has been held to protect a “private space in which man may become and remain himself”. The ability to do so is exercised in accordance with individual autonomy’. If such an expansive approach were to be adopted by the Indian Supreme Court, it could develop into something like the ‘right to informational self determination’ of the German Constitutional Court (Greenleaf, 2009a). But this has not yet occurred. Indian constitutional law does not provide data protection as yet, and nor does its tort law provide protection to privacy.

In relation to the surveillance systems discussed in this article, it is particularly important to note that there are no provisions in current Indian law restricting interconnection of files, either in the public sector or the private sector. On the contrary, the *Right to Information Act 2005* (RTI Act) s4(1)(a) requires all public authorities to:

maintain all its records duly catalogued and indexed in a manner and the form which facilitates the right to information under this Act and ensure that all records that are appropriate to be computerised are, within a reasonable time and subject to availability of resources, computerised and connected through a network all over the country on different systems so that access to such records is facilitated;

This legislative requirement is not balanced by any data protection law placing limits on such ‘linking up’ in the case of personal data. If such a ‘linking up’ of all records of public authorities was in fact undertaken, rather than just being legislative wishful thinking, then it would be extremely dangerous to Indian citizens in the absence of the protections of a full-fledged data protection law. Even with such a law, the advisability of interlinking all such records is very questionable. There does not seem to be evidence that it is yet occurring in the unrestricted way anticipated by s4(1)(a), but in the absence of other legislative prohibitions, s4(1)(a) gives public authorities the imprimatur to network record systems, ostensibly to facilitate the access right, but it could be just as easily turned to data matching and similar surveillance uses.

The development of data protection laws in India, when it finally does occur, will only be able to be understood in light of the development of these government surveillance systems and their intersection with private sector activities.

2 India's converging data surveillance context

The second vast surveillance project is the National Population Register (NPR) of persons resident in India, which is to be a by-product of, but separate from, the Census data collection commencing April 2010. NPR is eventually intended to lead to the issue of national identity cards based on citizenship (not just residence) and a National Register of Citizens. The third is the National Intelligence Grid (NatGrid), a centralised data system, which is intended to amalgamate and integrate data forwarded by 21 government agencies and departments, partly for anti-terrorism purposes. If the three projects sounds confusing and overlapping, that's because they are. These are to some extent competing proposals by different agencies, but they have obvious potential for convergence. The implications for Indian's future as a liberal democracy are significant. The second and third projects, and the MNIC (a precursor to the UID), will now be summarised so that their potential relationships to the unique ID number project can be better understood. These are not the only mass surveillance systems under development in India. A DNA database has been proposed by the Home Minister (Ramanathan, 2010a), and a compulsory network of credit reporting bureaux is being developed under the *Credit Information Companies (Regulation) Act 2005* and the close supervision of the Reserve Bank of India (Greenleaf, 2010: Part II(2)).

2.1 National Population Register (NPR)

The India census commenced on 1 April 2010 with house-listing operations and will conclude with the attempt to identify every person in India on March 1 2011. Announcing the Census schedule, Union home secretary G K Pillai confirmed the government's intention to proceed with the National Population Register. The NPR, to be developed from data collected simultaneously with the March 2011 census data, but ostensibly separate from it, is intended to record 15 items about each person, primarily to do with identity (including a photograph and 10 fingers biometry of persons above 15 years). R Gupta (2010a) states that NPR will include name, sex, date of birth, current marital status, name of father, mother and spouse, educational level attained, nationality, occupation, activity pursued, present and permanent addresses along with individual biometrics'.

The NPR is intended to show that a person is a resident of India, not their citizenship, but is also intended to be used later to develop a National Register of Citizens and identity cards to be issued to citizens above the age of 18 years, 'after weeding out all illegal immigrants who might have got entry into the NPR by any means' (Mohan, 2010). R Gupta (2010a) says 'Chidamabaran has cautioned that due care needs to be taken to ensure that "illegal" residents in border districts (Bangladesh, Nepal) don't worm their way into the NPR giving the census an ominous policing quality'.

The *Citizenship Act* (as amended in 2003) and the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003 require the Registrar General of India to establish both a Population Register and a Register of Citizens, and this is considered to mean that the latter is a subset of the former (Pillai, 2010). It is important that the NPR is being created under the *Citizenship Act*, not the *Census Act 1948*, because the latter contains express confidentiality provisions (s15) but the former does not (Ramanathan, 2010).

Although C Chandramouli (registrar general and census commissioner) stresses that the Census and NPR are separate and 'we are collecting data for these two together just to save time' (Chatterjee, 2010), this census collection is explicitly not only about providing statistical information to the public or to other agencies. Chandramouli admits that

'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. As NPR and UID involve biometrics, there is no way a person can issue more than one identity card or enrol twice. Also, we will publicly display the primary list in villages. Then, it will be sent to the gram sabha before being sent to the UID authority. Thus, the village itself will be able to do the primary scrutiny and tell us if there is something wrong' (Chatterjee, 2010).

As R Gupta puts it 'The NPR will depend on UID for de-duplication' (2010a). Whether the NPR will also be provided with a person's UID number and be able to store that is unknown.

Asked whether the census would include questions on caste, Chandramouli stated 'In independent India, there has never been a census where details related to castes were given. We don't have that mandate from the government' (Chatterjee, 2010), confirming earlier comments by Pillai. However, in May 2010 Finance Minister Mukherjee announced that the 2011 Census would require Hindus to record their caste, for the first time since the British-administered census of 1931, and this has occurred. Minister Pillai states that the census collectors will simply record the caste information provided to them by householders, but will not be 'an investigator or verifier' (Pillai, 2010). Whether the NPR will also permanently

identify individuals by their caste, as one of the 15 items recorded about each person, is not yet clear, but it would clearly be a very sensitive privacy issue if this was done. The sensitivity will be increased by any links between the NPR and the UID system.

2.2 National Intelligence Grid (NatGrid)

The National Intelligence Grid (NatGrid) is reported to have received the go-ahead from prime minister Manmohan Singh, after a meeting of the cabinet committee on security, with an official announcement on its formation also expected by June (H Gupta, 2010), though others state that no final decision has yet been made (Ramanathan, 2010). The NatGrid project is promoted by Union home minister P Chidambaram, who was also instrumental in the creation of the National Investigating Agency (NIA) to coordinate and act on intelligence inputs on terrorism. According to reported sources (Gupta, 2010), data from 21 government agencies and departments, and private sector bodies, is to be forwarded to the NatGrid for integration. These sources have variously been described to include 'Pan card, voter ID card and ration card details, income tax returns, degrees obtained from schools and colleges, bank account numbers, financial transactions, travel documents, passport details, police stations and jails across the country among others' (R Gupta, 2010) and 'railway and air travel, Income Tax, phone calls, bank account details, credit card transactions, visa and immigration records, property records, driving licence' (R Gupta, 2010a). R Gupta also claims that 'NATGRID is expected to be fully operation by May 2011 and will eventually use UID numbers for these inter-database linkages', and is to be used 'for real-time monitoring of all residents in the country' (R Gupta, 2010a).

2.3 The Multipurpose National Identity Card (MNIC)

Before examining the UID number development, it is necessary to first look briefly at its very recent precursor, now apparently abandoned. A universal ID scheme for India has had a decade-long gestation, first proposed by the National Democratic Alliance Government in 2001 as the Multipurpose National Identity Card (MNIC), and approved by the government in 2003 (UIDAI 2009: p4). The MNIC project was an ID card project based on 'smart card' technology, and passive RFID (Mehmood, 2008). It had reached pilot project stage by 2007 but, despite the issuing of pilot scheme cards in various districts and sub-districts (listed in Wikipedia 'Multipurpose National Identity Card' entry, 2010), the issuing of cards has apparently stopped, and the energies of the government have shifted to the UID scheme. Apart from the fact that the UID scheme is not based around the issuing of an ID card, there is another fundamental difference in that the MNIC was based on citizenship, not residence, and it is claimed that the cards would have been 'the first citizenship document of its kind in the country' (Mehmood, 2008:113).

The origins of the MNIC proposal are said to be in the Kargil War between India and Pakistan in 1999 over disputed border territory in Kashmir. The report of the Kargil Review Committee (2000) recommended the issue of ID cards to 'border villagers in certain vulnerable areas' and that this would be relevant in some other areas of India with disputed borders (Mehmood, 2008: 114). Its origins therefore lay in security concerns.

This time around, the ID card and citizenship aspects have both ostensibly been dropped, with the emphasis on a unique ID number and residence. 'While the MNIC project suffered from the image of being principally a doubtful internal security measure ... the UID project has been packaged and promoted as primarily a mechanism to improve the delivery of government schemes to the poor and marginalised' (*The Hindu*, 13 Nov 2009). We now turn to the details of the UID.

3 The Authority: Establishing the ID number system

First, who will operate the UID scheme, and in particular the Central Identities Data Repository (CIDR), the intended register for identity information on 1.2 billion people?

3.1 The UIDAI or 'National Identification Authority of India'

The Unique Identification Authority of India (UIDAI) is currently attached to the Planning Commission. Its Chairman is Nandan Nilekani, former head of Indian IT success story, Infosys. Nilekani has a Cabinet-level appointment, and there is a Cabinet Committee on the UIDAI.

The Bill will rename UIDAI as the 'National Identification Authority of India' (s11). It will consist of a Chairman and two part time Members appointed by the Central Government for three year terms and eligible for reappointment (ss12, 14). The members of the Authority can only be removed for reasons of insolvency, incapacity, convictions, conflict of interest or 'in the opinion of the Central Government', abuse of position so that continuation would be 'detrimental to the public interest' (s15). The Central Government may give the Authority written directions on 'questions of policy, other than those relating to technical and administrative matters' (s50). The Authority can also be 'supersede' the authority for up to six months, and appoint someone else to run it (s48). The independence of the Authority is therefore very limited. Some Indian commentators have called for it to be an autonomous body, answerable only to the Courts, and for s48 to be repealed (Gupta, 2003b).

The Authority will be empowered to make Regulations under the Act, whereas the Central Government is empowered to make Rules under the Act (ss53-54). Such Rules and Regulations are disallowable by Parliament (s55). The Central Government may also, during the first two years of the Act, make orders not inconsistent with the Act, to remove difficulties in giving effect to the Act's provisions (s57). Such orders must be laid before Parliament (s57(2)), but do not seem to be disallowable.

3.2 Outsourcing India's identity repository?

The Central Identities Data Repository (CIDR) may be operated by the Authority or it may outsource its operation (s7, anticipated by UIDAI 2009: p32). There is no provision preventing it being outsourced to private sector entities or to foreign entities, and no need for regulations, therefore no capacity for Parliamentary disallowance. In theory, it could even move the CIDR offshore, though this might be expected to result in a written direction from the government under s50. It seems extremely convenient that what would probably be the world's largest outsourcing contract has been removed from Parliamentary scrutiny. In contrast UIDAI may also outsource any of its other functions, but must do so by (disallowable) regulations (s7). The Authority can enter into a MOU or agreement with agencies of any government in India for the purpose of carrying out any of its functions including authentication (s23(3)), so there is considerable, and confusing, scope for powers to be divested. A major role of the Authority will be in supervising 'the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act', by calling for reports, inspections and audits (s23(2)(i)).

So who will be in charge of particular aspects of India's ID system day-to-day remains to be seen.

4 The unique ID number (aadhaar)

We now consider how the number is to be constituted, its coverage, whether obtaining one will be voluntary, and what entitlement individuals have to a UID.

4.1 Randomness as privacy and freedom

The ID number (to be called an 'aadhaar number': s2(a)) will be a random number (s4(2)), with no meaningful information relating to the holder built into it (sex, address, DOB etc). It is intended to be 12 digit, with up to 4 additional digits as a check sum (Nilekani, 2009). The randomness of the number is an important privacy protection, as it does not reveal personal information simply through use or disclosure of the number. In contrast, in China's 18 digit ID number '[d]igits 1-6 ... represents the cardholder's administrative unit, 7-14 for the ... birth year (4 digits), birth month (2 digits), birth day (2 digits); 15-18 code assigned to persons that share the same birth date and lie in the same district or county, with the second to last digit as an even number for female and an odd number for male' (Brown, 2008:59). The last digit is presumably a check sum.

The randomness of the Indian UID reinforces that freedom of movement exists in India (*Constitution of India*, A 19⁴). The UID (or a card that displays it) will therefore not act as an 'internal passport', able to be used to check and control whether people are where they are supposed to live, have permits to work in cities and other forms of control of freedom of movement. In China, where internal freedom of movement is limited, the location information inherent in the ID number can be used to reinforce those limitations⁵.

4.2 From birth to 'inoperative'

Numbers will be allocated to anyone who is a resident of India (s3(1)), not just citizens (as with the MNIC), but the government can also issue it to classes of non-residents (s3(1)). Children will be eligible to obtain numbers from birth, but their numbers will be linked to a parent's biometrics until they are old enough to provide their own (from 5 years of age). It is proposed that the Registrars of Births Deaths and Marriages should carry out the registration of all new-born children, and record their UID in their birth certificates. Likewise, they should ensure that the UIDAI records are altered to mark a deceased person's UID as 'inoperative' (UIDAI 2009, p22).

4.3 Between pseudo-voluntary and compulsory

Obtaining a UID is stated to be voluntary in all UIDAI publications, and this is implied by the Bill ('Every resident shall be entitled to obtain an aadhaar number': s3(1)). Otherwise, the Bill gives the Authority powers of 'generating and assigning aadhaar numbers to individuals' (s23(2)(d)).

An obvious exception to voluntariness is that children's UIDs will hardly be voluntary if allocated at birth. Furthermore, UIDAI states that 'however in time, certain service providers may require a person to have a UID to deliver services' (UIDAI 2009a: FAQ 10), and that both governments and Registrars (public and private sector) 'may mandate enrolment' by their clienteles (UIDAI, 2009: p6). There are no prohibitions on such demands in the Bill, nor in any data protections laws in India. There is no general prohibition on private sector bodies demanding UIDs as a condition of service, though it is not possible to generalise and there may be exceptions in some regulated sectors of the Indian economy.

Given these statements and the privacy lacunae in Indian law, all that the UIDAI's claims of voluntariness amount to is that, while the Authority will not decide for whom, and when, UIDs

⁴ Article 19(1) provides, *inter alia* 'All citizens shall have the right - ... (d) to move freely throughout the territory of India; [and] (e) to reside and settle in any part of the territory of India'. The right only applies to citizens, not residents.

⁵ See Brown, 2008:61-63 for the relationship between the ID card and the *hukou* (household registration) system in China in relation to freedom of movement.

are to be compulsory, any of India's 36 Central, State and Territory governments may do so. It remains to be seen whether the myriad of proposed public sector and private sector Registrars will accept mass involuntary registrations of individuals by supply of data from other databases, or 'mandate enrolment' as UIDAI suggests. The position is unclear, but it seems likely that, for most residents of India, the UID will become mandatory over time, unless they voluntarily register before then. It is likely to be best described as somewhere between compulsory and 'pseudo-voluntary'.

4.4 Entitlement without rights

The 'entitlement' to a UID is that the Authority 'shall ... issue' a UID after it verifies the demographic and biometric information provided in relation to a person (s3(2)). Getting a UID will only, on the face of the Bill, entitle a UID holder to be 'authenticated' under s5 as to their identity (discussed later), and 'shall not, by itself, confer any right of or be proof of citizenship or domicile' (s6).

There are no specific rights of appeal provided in the Bill which will operate where the Authority fails or refuses to issue a UID, or where a person and the UIDAI dispute the person's 'entitlement'. The only relevant provision in the Bill is that the Authority has powers for 'setting up facilitation centres and grievance redressal mechanisms for addressing grievances of residents' (among others) (s23(2)(s)). No matter how well-intentioned these measures are, they will still only amount to 'internal review' (or Caesar appealing to Caesar).

Given the importance that the UID is intended to have in Indian life, particularly for the underprivileged, it seems obvious that there needs to be some form of external review. At present, the 'entitlement' can only, it seems, be enforced by resort to general provisions of Indian administrative law. How long does it take to get such a matter before the Indian courts? Can the underprivileged classes who the UID is intended to assist afford counsel? Perhaps the Ombudsman (Lokpal) can help. It is extraordinary that there is no 'built-in' right of appeal to a specialised Tribunal against refusal to issue a UID⁶. After all, this is an Authority that is supposed to have 1.2 billion customers in due course. One obvious candidate is the Central Information Commission, a very active tribunal which has made more than 33,000 decisions enforcing the *Right to Information* legislation⁷.

While the UID is presented as a benefit to the underprivileged, those who are refused one may find that they are even more underprivileged, once it starts to become required for transactions. As matters stand, this Bill lacks due process guarantees and is a recipe for an unnecessarily authoritarian Authority.

4.5 'Special measures': Identifying tribals, itinerants and the disabled

As Lyon and Bennett (2008:9) note 'Once cards are mandatory, then they may be used to single out or even to harass visible minorities and those with alternative lifestyles'. In the most notorious case, the inclusion of ethnic identity on ID cards in Rwanda in the 1990s was an instrument of genocide⁸, perhaps the most significant single factor in its speed and

⁶ Chapter V of the Bill establishes an 'Identity Review Committee' but it has no function except to 'establish the extent and pattern of usage of the aadhaar across the country' (s29).

⁷ Central Information Commission website <<http://cic.gov.in/>>; The CIC's decisions are also conveniently searchable on AsianLII at <<http://www.commonlii.org/in/cases/INCIComm/>>.

⁸ The International Criminal Court has heard expert evidence that "During the colonial period, the ID became a passport to success for Tutsis, but during the genocide it became their death certificate" – see '[Rwanda](#): ID Cards

magnitude (Fussell, 2001), and during the Nazi era in genocidal actions against Jews, Gypsies (Roma Sinta), and others (Fussell, 2001). The potential for abuse against marginal groups also needs to be guarded against in relation to ID numbers, and the contents of ID registries. Fussell (2001) also notes that 'group classifications on ID cards also played important roles in facilitating the large-scale expulsions of tens of thousands of persons on account of their group identity from Bhutan in 1991 and Ethiopia in 1998', and documents many other examples of mass expulsions, forced relocations, and group denationalisations involving ID cards.

Fortunately, the UID will not directly facilitate India joining the more than 20 countries where ID cards state 'an ethnic racial or religious affiliation' (Fussell, 2001). Information cannot be collected on a person's 'race, religion, caste, tribe, ethnicity, language, income or health' (s2(h), s9), presumably because of the potentially discriminatory uses of this information.

The supposedly beneficial nature of the UID, to enable individuals from disadvantaged groups to more easily authenticate who they are, is reflected in the requirement that 'The Authority shall take special measures to issue aadhaar number to women, children, senior citizens, persons with disability, migrant unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations' (s10).

There could not be 'special measures' which involve collecting the demographic information prohibited by s9. But if 'special measures' are being taken to enrol members of a specific 'nomadic tribe', are there not risks of discriminatory actions being taken? Are 'persons with disability, migrant unskilled and unorganised workers, nomadic tribes' or itinerants (such as the Bauls of Bengal) necessarily going to feel encouraged by the endorsement in s10 that 'special measures' should be taken to identify them? Given that the voluntary nature of the UID scheme is likely to be illusory, it could be expected that they would be far more reassured if s10 was coupled with a provision that under no circumstances could they be required to obtain a UID.

The history of ID schemes in other countries is punctuated with episodes of their use for genocide or lesser forms of discrimination and oppression. India's history is punctuated by episodes of communal, ethnic and religious violence. Special measures are needed to ensure that any ID system in India is not, and as far as possible, cannot be, misused in this way. The lack of such measures in the current Bill could become its dark side.

5 Biometric and demographic data to be collected

Next we turn to what information is to be collected by UIDAI on each individual. 'Identity information' in the Bill means the biometric information, demographic information and aadhaar number held about each individual (s2(k)).

5.1 Biometric information

The 'biometric information' which UIDAI may require from a UID applicant 'means a set of such biological attributes of an individual as maybe specified by regulations (s2(e)). Since the Authority can decide for itself from time to time what biometrics can be required, this is not fixed at all, and may expand over time.

Became Death Certificates During Genocide, Says Expert', *allAfrica.com*, 1 March 2006 at <<http://allafrica.com/stories/200603020402.html>>

The original outline of the UID system only refers to the collection of 'photograph' and 'finger prints' as biometric data to support identification (UIDAI 2009: p11). However, the biometric aspects have already escalated following a report in December 2009 (UIDAI 2009b) by a UIDAI committee Chaired by Dr BK Gairola, Director General of India's National Informatics Commission. NIC recommended collection of three biometrics and standards for their collection: 3 photographs (so as to support automated face recognition to supplement a primary use of fingerprints, not only for visual comparisons); 10 fingerprints (to support 1:N matching in enrolment de-duplication, although not needed for 1:1 authentication); and 2 eye iris scans if the UIDAI 'feel it is required' in order to achieve a high enough level of de-duplication. UIDAI's biometrics committee has recommended that iris scans be taken to attempt to overcome 'the risk that fingerprints might not be sufficient to ensure uniqueness', and because they are more reliable at a younger age than fingerprints of children (UIDAI, 2010).

Therefore, there has already been a significant escalation in all three biometrics from the original specifications (the third not being originally included at all). What further expansion is likely? The legislation places no limits on this other than the possibility of Parliamentary disallowance: 'function creep' has been built in.

5.2 Demographic information

The 'demographic information' which the UIDAI can require is similarly open-ended. It 'includes such information relating to the name, age, gender and address of an individual (other than race, religion, caste, tribe, ethnicity, language, income or health), as maybe specified in the regulations for the purpose of issuing an aadhaar number' (s2(h)). The limits on demographic data to be collected indicated by s2(h) are confirmed by s9: 'The Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health'.

Since 'demographic information' can include any characteristic of a human population, and the exclusions are not related to any of the inclusions, it is hard to see that principles of statutory interpretation would place any other practical limit on what the regulations could declare to be 'demographic information'. For example, it could include criminal history, or sexual orientation, or political affiliation. UIDAI expected its enabling law to 'contain a proscription against collecting *any other information* than the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters' (UIDAI 2009: 32). This has not occurred in the Bill, which delegates such questions to regulations made by UIDAI. As is common, protective measures foreshadowed by system proponents when they are selling the virtues of their scheme fail to eventuate. An overly-broad definition of 'demographic information' could be disallowed by Parliament, or declared unconstitutional by the Supreme Court (see Greenleaf, 2009a), but these safeguards would be less necessary if poor drafting had not enabled such function creep in the first place. As UIDAI originally proposed, the Bill should specify precisely what demographic data the Authority can collect, and prohibit it from collecting any other.

The demographic data to be collected by the UIDAI, according to their original explanation, was only to comprise name, date of birth (DOB), gender, names of father and mother and (optional for adult applicants) their UIDs; address (permanent and present) (UIDAI 2009: p6). However, the December 2009 report of the demographic committee (UIDAI 2009c) adds 'mobile number' and 'email address' as option data fields for collection. Because of their function as location devices they are potentially sensitive personal information. The report also points out that the collection process will require, for the first time, the reduction of both

Indian names and addresses into a standard format. As yet, what the regulations will contain is unknown, and in any event they can be changed from time to time.

6 The number allocation process

What is the process by which this information is to be collected, and UIDs then allocated?

6.1 Registrars, enrollers and introducers

A feature of the registration process in the Indian system is that a wide variety of third parties from both the public and private sectors will be appointed by UIDAI as 'Registrars', with the primary function of introducing residents who ('voluntarily') wish to obtain a UID. 'Registrars will process UID applications, and collect to the CIDR [Central ID Data Repository] to de-duplicate and resident information and receive UID numbers.' UIDAI describes it as 'A partnership model: The UIDAI leverages the existing infrastructure of government and private agencies across India.' (UIDAI 2009: p5). The idea seems to be that government agencies (at all levels) and companies (banks, telcos, insurers etc) will act as 'enrollers', using their existing 'client' databases to bring very large numbers of UID 'applicants' to UIDAI's registrars, and will in most cases perform the collection of the biometric and demographic data to be forwarded to UIDAI's CIDR for de-duplication. They will verify the demographic information by inspection of Proof of Identity (POI) documents, or by obtaining verification from 'Introducers' (who have a UID) and who can vouch for the applicant. They will then (after the de-duplication process by the CIDR) provide these 'applicants' with the tokens containing their UID (discussed below). None of the details of these processes or the relationships between these parties will be clear until the Regulations are made.

Gupta (2003b) raises a number of situations where the registration process could be abused against the less powerful, including enrollers placing requirements of continuing association as a condition of obtaining a UID, and organisations denying essential services unless a person first obtains a UID (even though they have alternative identification).

6.2 Registration process

The CIDR collects the applicant's biometric and demographic data from the relevant Registrar (but not the POI behind the data except for the name and UID of the Introducer, if any). It then 'de-duplicates' the data, which means checking whether there is already a person in the CIDR database with the same biometrics. Once approved, CIDR issues a letter stating the person's UID and recorded biometrics and demographic data, to the relevant Registrar, for delivery to the UID applicant.

6.3 Cash incentives for enrolment

Registrars will not be prevented from making the obtaining of a UID a condition of provision or continuation of the services they provide (in the absence of data protection laws providing otherwise). It therefore seems that their role will not always be a matter of facilitating genuinely voluntary applications. It seems that Registrars will also be able to charge for their services (UIDAI 2009: p6), but the fees for doing so will be set by the UIDAI by regulations (s54(2)(s)). The procedures by which they can, in effect, simply require all their clients to enrol, are yet to be clarified.

Other organisations than Registrars may also act as 'enrollers', who 'will interface with people seeking UID numbers' and bring them to Registrars with the necessary information or 'Introducer'. The Authority will apparently also set the fees they are able to charge.

The government will also provide financial incentives of around US\$2.50 to some potential UID holders: 'People living below the poverty line will get Rs 100 each as they are allotted the Aadhar number [sic]. The Finance Commission has made a grant of about Rs 2,980 crore for the incentive for getting registered in the Aadhar scheme for people who might forgo a day's income to travel and get themselves enrolled' (*Economic Times*, 2010).

The potential combination of compulsion to obtain UIDs and substantial amounts of money (if the numbers of UID holders is large enough) both being paid by UIDAI and chargeable against some UID applicants, could become a dangerous mix of moral hazards and conflicts of interest, particularly if at any time it becomes coupled with the UIDAI imposing pressures to increase the numbers of enrolments. This needs to be handled carefully, and perhaps for there to be less discretion in the hands of the UIDAI than at present.

7 Uses of UIDs and CIDR data by UADAI

Once the identity information is collected, and a UID allocated, what can UADAI do with the information it holds? The Central Identities Data Repository (CIDR) will contain the demographic and biometric data described above, but no other data.

7.1 Authentication

According to UIDAI's planning documents, the CIDR would be used for two purposes only: 'de-duplication' in the enrolment process (discussed above), and authentication to CIDR users (UIDAI 2009: p24). But there is a lot packed into those two purposes. To provide online authentication to a CIDR user (public or private sector) that an individual has the UID that they claim to have, but only by a 'Yes' or 'No' response, and without the sharing of any data in the database (UIDAI 2009: p7). The database users will provide to the CIDR biometric and demographic data in varying combinations, allowing authentication of various degrees of strength.

The Authority is given the powers and functions to do these things both generally (s23(1)), and in 20 enumerated categories (s23(2), more than half of which must be carried out by regulations and are thus subject to Parliamentary oversight. For the rest, the Authority will simply have power vested by the Bill. There are therefore many details not yet known. There is, however, specific power for the Authority to 'perform authentication', which is defined (s2(d)) as

"authentication" means the process wherein aadhaar number, along with other attributes (including biometrics) are submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness thereof on the basis of information or data or documents available with it;

The Authority is then required to 'respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic information and biometric information' (s5(2)).

7.2 An updated population register

To the two stated uses above we need to add a third distinct use of CIDR: to continuously update it. It is important to stress that CIDR is not intended to be static, holding *historical* information about an individual correct at their date of enrolment (or re-enrolment). Far from it, the Bill provides that "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' (s8). A number of issues arise from this provision. First, no penalty for failing to comply with such a requirement is stated in the Bill.

The requirement to update demographic information is most frequently an obligation on a person to update their address. Name and gender change infrequently, and age can be calculated. This means that Indians will have for the first time a general obligation to inform the government every time they change their location. As a surveillance measure, this is one of the most potentially intrusive and significant steps a government can take. If mobile phone number and email address end up being included, as has been proposed, it could also provide the key information needed to keep individuals under surveillance, if this was sought. The requirement to update biometric information means that, even though the biometrics required to obtain a UID are limited, once you have one you can be required to come back in and provide additional biometrics if the requirements under the Act change. Gupta (2003b) proposes deletion of s8, arguing that 'since identity is linked to biometrics [in the authentication process] updating doesn't serve any purpose linked to obtaining welfare services'.

7.3 Privacy protections concerning CIDR

Chapter VI 'Protection of Information' of the Bill is a rudimentary data protection code, given that India has no data protection law of significance other than a law in relation to credit reporting (not yet effective). The Authority is required to ensure the security and confidentiality of identity information (s30(1)), and to implement security safeguards to protect against loss or unauthorised access, use or disclosure (s30(2)). In India's data protection vacuum, any protective provisions are of some value, but these are not fully-developed data protection provisions because they are not accompanied by any mechanisms by which individuals may insist that suspected breaches are investigated and if necessary compensated. There is also a general prohibition against the Authority or any of its staff revealing any information in the CIDR (s30(3)), which is of course overridden by the specific authority to respond to authentication queries in s5.

The Authority must keep records of all such queries and its replies (s32), and make this information available to UID holders on request (s32(2)). Where UID holders claim that their demographics or biometrics as recorded by the Authority are wrong or have changed, they can request the Authority to change them (s31). But there is no independent tribunal before which UID holders can enforce these ostensible rights. In contrast, individuals would also have right to access (but not to correct) their demographic and biometric information under India's *Right to Information Act 2005*. This is a right enforceable through appeals to the Central Information Commission. The Bill is once again deficient in not providing due process.

7.4 Exceptions to the prohibition on disclosures from CIDR

The only stated exceptions in the Bill to the prohibition on disclosures of identity information in the CIDR are for disclosures pursuant to an order of a competent court (s33(a)), or approved by a Minister, pursuant to a direction by a Joint Secretary or equivalent 'made in the interests of national security' (s33(b)). UIDAI expected its enabling legislation to contain a prohibition of 'the facilitation of analysis of the data [by UIDAI] for anyone or to engage in profiling or any similar activity' (UIDAI 2009: 32, 34). This does seem to be the effect of the draft Bill. It remains to be seen whether the legislative process will continue to exempt CIDR from all laws concerning, say, requests for data concerning criminal suspects, where perhaps the authorities hold fingerprints of a suspect but no other identifying data. Will the Authority be able to deny them access to the fingerprint matching which could disclose the name, addresses, photo, telephone number and email address of such wanted persons? It is also not

unreasonable to ask whether, even if the first version of the legislation does do this, will it continue unamended? However, when compared with many data protection laws, the current exceptions in the draft Bill are restrained and should be considered 'pro-privacy' in their restraint.

Gupta (2003b) proposes deletion of s32, arguing that when considered in conjunction with s33(b) (allowing some accesses to CIDR for national security purposes), it is 'tantamount to tracking of individuals by the state'. However, without the logs of authentication requests kept under s32(1) individuals would not be able to find out which organisations have attempted to authenticate their identity, and this would reduce their capacity to monitor potential abuses of the ID number. The access logs do raise the risk of tracking of individuals, but this might be better addressed by further limiting or deleting (as Gupta also proposes) the 'national security' accesses under s33(b).

But the s33 accesses are not the whole picture of CIDR accesses, because the Authority is also empowered to undertake 'sharing, in such manner as may be specified by regulations, the information of aadhaar number holders, with their written consent, with such agencies engaged in delivery of public benefits and public services as the Authority may by order direct' (s23(2)(k)) and to 'specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations' (s23(2)(h)). There is nothing in the Bill or elsewhere to ensure that such 'consent' is not in fact a condition of provision of such benefits.

This pseudo-voluntary 'data sharing' only applies to the public sector. In addition, and applying to both the private and public sectors, there is a potentially very dangerous provision that an UID holder 'may request the Authority to provide access to his identity information in such manner as may be specified by regulations' (s30(3) proviso). Depending on what the regulations say, this provision could provide a 'back-door' entry for agencies and companies to obtain copies of the demographic and biometric data held on CIDR, a process usually called 'forced access' and regarded as very anti-privacy.

So, while the Bill does not provide for mass data matching of the whole clientele databases of other government agencies against the CIDR, provided agencies are patient they can obtain much the same result through pseudo-voluntary individual consents to the disclose of demographic and biometric data. It can be on a regular basis, if UIDAI's regulations allow this.

7.5 Criminal penalties and compensation for abuses

UIDAI intended there to be a wide range of penal provisions against parties who do not comply with the Act, against improper disclosures of information by parties involved in the system, and against individuals who provide false information or who attempt various forms of identity fraud (UIDAI 2009: p33). These are now provided in Chapter VII in considerable detail. The offences under the *Information Technology Act 2000* (as amended in 2008; see Greenleaf, 2009) will also apply to the CIDR.

Summarising proposed legislative protections in March 2010 D Mogilishetty (Legal Advisor, UIDAI), in response to questions (Gupta, R, 2010), outlined the proposed criminal offences, but did not mention individuals affected being provided with a right of action for compensation in the event of any of these abuses taking place. Nor was there any mention of the compensation provisions in s43A of the *Information Technology Act* (not yet in force) applying here. However, Mogilishetty did state that UIDAI would not have any responsibility for denials of service by service providers based on failure to identify, or for use of the UID data for data matching: 'Convergence of existing databases will need to be addressed and

governed under a larger data protection regime applicable to the whole country and therefore this is a matter beyond the mandate of the UIDAI'. These comments illustrate how limited is the scope of the privacy protections offered by the draft Bill: even potential (non-criminal) misuses of the UID will not be covered.

8 Use of the UID number and ID tokens by others

How will the UID and identity information (demographics and biometrics) be used by those outside the Authority? First is the obvious use, that anyone will be able to make 'authentication queries' about a UID-holder (and get a yes/no answer). Second are the public sector 'data sharing' uses, and the private/public sector 'forced disclosures', already discussed. Third is the way in which ID cards will in fact be issued. Finally, inclusion of the UID in other databases must be considered. We consider the last two here.

8.1 Let a thousand ID cards bloom

The UIDAI says it will not issue ID cards, but the truth is it will issue something very like one, which may become a 'poor man's ID card' in some circumstances.

Once the UID number is assigned, the Authority will forward the resident a letter which contains his/her registered demographic and biometric details. This letter will also have a tearaway portion which has the UID number, name, photograph and a 2D barcode of the finger print minutiae digest. ((UIDAI 2009: p14).

Registrars in both public and private sectors will however be encouraged to issue higher integrity ID cards containing the UID and the biometrics collected for the purpose.

If the Registrar issues a card to the resident, the UIDAI will recommend that the card contain the UID number, name and photograph. They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/store the biometric collected from the applicant on the issued card. If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification. But the UIDAI will not insist on, audit or enforce this. (UIDAI 2009: p32).

UIDAI expected regulations would govern 'information to be visible on the card to be issued by the Registrar, as well as the look and feel of the card.' (UIDAI 2009: Ch 6 Legal framework). The Bill does not mention this specifically as a subject of regulations, but its powers are broad enough to cover it. This approach could be seen as both a partial privatisation of the national ID system (the card part), and a significant incentive to commercial organisations to become Registrars, particularly since they will be able to charge fees for their role in registration.

Some significant privacy issues remain unresolved. It seems that not only will the UIDs of residents be compulsorily included on multiple types of ID cards, letters etc, but so will their supporting biometrics, with no restrictions on those to whom they produce them recording and using all of the identifiers. The privacy implications of this are likely to be complex.

For example, the Bill says nothing about protection against demands to produce an ID card (either the letter token issued by UADAI, or an alternative). Gupta (2003b) considers that there needs to be protection against non-possession becoming 'grounds for detention', but her reasons are not stated.

8.2 Inclusion of the UID in other databases

The core idea behind the UID scheme is that 'The UID will become the single source of identity verification. Once residents enrol, they can use the number multiple times – they would be

spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on.' (UIDAI 2009: p7). UIDAI wants agencies involved in the delivery of services to 'authenticate a resident's identity against the UID database every time they carry out a service transaction' (UIDAI 2009: p8). The databases operated by Registrars for their own activities may rapidly become populated with UIDs as a result of their role in the registration process (see above). However, the databases of non-registrars will also increasingly have records identified by UIDs as individuals provide them in order to have their identity authenticated against the UID database.

The consequence of these two developments, although it is nowhere acknowledged by the UIDAI, is that all service providers, whether Registrars or not, and whether in the public sector or not, will increasingly have the capacity to carry out data matching among their respective databases, using the UID as the common key. There are no privacy laws in India at present which restrict or control such data matching. The UIDAI can claim that it will not use the UID to carry out data matching, profiling etc, but it is providing other organisations with the essential tool to do so to an extent that they cannot do at present. UIDAI's consultants on the numbering scheme have recommended legislation to control the display and communication of UIDs (Kanakia et al 2010), but there is nothing in the Bill about this. Instead, the use of the UID is designed to be out of control.

8.3 Repeated requirements to document identity?

A number, or a token recording it, does not in itself provide the necessary link to a person. The UIDAI proposes that agencies and companies make various uses of the UIN and the tokens recording it. At the weakest, offline authentication, they simply compare the person visually with the photo on the token. The potential for fraud is considerable with such a low integrity ID token. Various forms of online authentication of higher but differing strengths are proposed in which combinations of the biometrics and demographics previously provided by the person are re-submitted for comparison with those in the UID database (UIDAI 2009, p25). This raises the prospect of persons from poor and underprivileged communities having to undergo repeated biometric data collections every time they wish to access a service. Instead of a 'full cycle of identity verification' based on paper POI, they may find a full cycle of biometric identification needed for authentication substituted for this. Will this be an improvement?

9 Conclusions and recommendations

There are many perspectives on ID systems that this article does not address, such as whether the claimed benefits to poor and underprivileged communities will result, whether the proposed biometrics can deliver the degree of de-duplication claimed or can be utilised under Indian conditions without causing misery to applicants that are no improvement on the paper systems they replace, where the benefits claimed for the system are likely to outweigh its costs, whether it can be delivered on its proposed budget, and whether the long-term dangers of misuse of a system such as this outweigh its potential benefits. Part of any of those analyses must include an understanding of the elements of the whole system that is proposed, and the legal constraints within which it is proposed it will operate. This article focuses only on the proposed legal regulation of the system, and in particular what controls there are on its scope, and the extent to which it protects privacy and provides due process. Ideally, there would be an independent privacy impact assessment (PIA) before a scheme such as this went ahead, but that is now unlikely.

9.1 'Designed to be out of control'?

In a study of the introduction of Hong Kong's 'smart' ID card, with the above title, I concluded (Greenleaf, 2008:90):

In the remaking of the Hong Kong ID card from 2000-2003 the Administration got most of what it proposed: a technically sophisticated smart ID card system; no defined limitations on the eventual expansion of the system; a system that was (modestly) multifunctional from the start; and the ability to expand many aspects of the system with little likely interference from LegCo in the form of disallowances or need for LegCo approval. It is an ID system that is out of the control of the semi-elected representatives and largely under the control of Hong Kong's mandarins.

These words have substantial application to what is proposed in India. There are few inherent limits on what the UID may be used for (other than the valuable limits imposed by randomness), and none defined as a matter of policy, though some may be subject to regulations. Most of the key details of how the system will work, or how extensive it will be, are left to regulations, so sporadic potential disallowance is the closest that democratic control will come to the system once the broad-brush Bill is passed. For example, what can be collected as demographics or biometrics is open-ended, definable only by regulations. UID holders will be able to exercise little control over abuses, as they are denied meaningful due process. The Bill designs this ID system for the benefit of the Indian bureaucrats who will run the UIDAI and administer the CIDR – or those to whom its operation is outsourced.

When bureaucrats and politicians build information systems which they can easily expand later, either without Parliamentary approval, or only with the rather remote risk of disallowance of Regulations, this does not necessarily mean that they have planned what the future expansions will be. What I said about Hong Kong's ID card is just as true of India's ID number (Greenleaf, 2008:80):

To warn of this risk is not to posit a 'function creep conspiracy'. It is likely that the authors of future function creep will have had nothing to do with the introduction of the smart ID card, they will merely be opportunistic beneficiaries of the loopholes that have been created.

I suggest that we have not yet seen anything like the final version of this system: governments tend to overestimate the simplicity and benefits of ID schemes when they first announce them, underestimate their dangers, and constantly re-design them 'on the run'. As for the legal environment, governments often fail to deliver the privacy protections proposed by system proponents.

9.2 *Fait accompli*?: Awareness, consultation and dissent

The UID has not yet become a significant party political issue in India, nor a matter of significant public disquiet. The consensus of political parties in India seems to favour these surveillance developments. Civil society organisations and individual activists are now starting to take up India's growing surveillance structure as an issue of civil liberties. This can be seen from a small but growing chorus of critical commentaries, and civil society forums organised by the Centre for Internet & Society and others (collected by Gupta, R, 2010). Media commentary in India is starting to note that the scheme involves risks, well summed up in a newspaper editorial: 'The attendant risks of such a potentially game-changing scheme – which includes risks of hacking, privacy invasion and the possible misuse of information by a future 'Orwellian' government – are real ... What it needs is a legal framework that enables the

creation of a unique identity system with adequate safeguards to protect privacy and confidentiality' (*The Hindu*, 13 Nov 2009).

Public consultation on the scheme and its legal framework is limited. The fact the UIDAI has allowed only two weeks for submissions on its draft Bill does not create confidence that it values consultation or outside input. The UIDAI has held meetings with civil society representatives on privacy and other concerns, but human rights lawyer Vrinda Grover subsequently stated that Nilekani and his team seemed to trivialise the human rights and privacy concerns, dismissing it as a 'conspiracy theory' (Jebaraj, 2010). Shekhar Singh, founder member of the National Campaign for People's Right to Information, who chaired one of the discussions at the meeting, is reported to have had similar misgivings (Jebaraj, 2010):

Mr. Nilekani initially seemed to shrug off responsibility about misuse, saying that the UIDAI was only concerned with providing the number, leaving the applications to others. 'I think there needs to be checks and balances,' Mr. Singh added. 'I do feel racial profiling and such misuses should be avoided... but I am not that sensitive to privacy issues,' he said, pointing out that India as a society was not very privacy-conscious. However, he also felt that the economic viability of the project and the justification of spending Rs.2,500 crore [US\$5 billion] on a project which may not be successful in preventing corruption should be vigorously debated. "No other country has implemented such a system. There should have been a discussion with the people before it was set up".

Critics of the UID, let alone opponents, obviously have a hard struggle ahead. However, ID schemes sometimes face unexpected and effective opposition, and are abandoned despite the expenditure of millions of dollars. This happened to proposals in Australia in 1987 (Greenleaf 1987) and 2007 (Greenleaf 2007 and 2008a), and most recently in the UK with the 2010 election of the Tory/Liberal government and the abandonment of their already-legislated ID card.

9.3 What is lacking in the Bill's privacy protections?

The question of whether it is good policy for India to have an ID system that is anything like the system currently being built by the UIDAI is considerably beyond the scope of this article. However, if we start from the assumption that some such system is going ahead, and therefore the legislation governing it should provide basic and internationally accepted levels of protection for privacy (including due process in decision-making concerning personal information), then the current scheme, and the draft *National Identification Authority of India Bill 2010* are deficient in that they lack at least the following protective provisions:

- (i) Outsourcing of the operation of the CIDR should be by regulations identifying the outsourcing provider, and thus disallowable (s7). Any movement of CIDR data outside India should also be by regulations.
- (ii) The Central Information Commission, or a similarly independent tribunal, should be empowered to adjudicate all disputes between the Authority and individuals.
- (iii) Individuals should be able to obtain compensation and injunctions for any breaches of their rights.
- (iv) The biometric and demographic information which can be collected by the Authority should be defined in the Bill, and collection of other personal data

prohibited. New legislation, and thus positive Parliamentary approval, should be required for any expansion.

- (v) The Bill should clarify whether obtaining a UID is compulsory or voluntary, and whether services may be denied to people because they do not have one.
- (vi) If the UID is voluntary, any special measures in relation to marginalised groups should also involve special steps to ensure that voluntariness is respected.
- (vii) Incentives given to any persons involved in the enrolment process should be designed to ensure that voluntariness is respected.
- (viii) UID holders should not be required to update their identity details unless this is necessary for the integrity of their UID and authentication. A continuously updated population register is not necessary for an ID number.
- (ix) The legislation should specify with which other agencies, and in relation to which benefits, the CIDR data can be shared, and any future changes should also be by legislation.
- (x) It should be prohibited for anyone to require a UID holder to obtain their CIDR data.
- (xi) It should be prohibited for any other databases to record the UID number.

Amendments such as these would not necessarily make the UID safe for India's 1.2 billion people, but they would reduce the risks of abuse. As India's economy and society become increasingly similar to those of other successful capitalist economies, the Indian government will increasingly need to adopt a full data protection law, as is the case throughout Europe and in an increasing number of countries in the Asia-Pacific. It has often been the case that the introduction of a new data surveillance system such as an ID card or a data matching system has shown the need – and provided the political trade-off – for the introduction of a full data protection law.

An optimistic point on which to conclude is the hope that this may also be the case with the enactment of an Indian Data Protection Act to accompany ID number legislation. It is not impossible, as India's UPA government is reported at the end of June 2010 to have 'set up a panel of senior officials of the rank of secretary to prepare a blueprint laying down the ground rules for privacy and data protection and fixing the criminal liability of offenders', with the aadhaar and Natgrid proposals identified as the two main precipitating factors (Makkar and Agarwal, 2010).

References

- Amoore, L (2008) 'Governing by identity' in Bennett and Lyon (2008)
- Bennett, C and Lyon, D (2008) *Playing the Identity Card* Routledge, 2008
- Brown, C L 'China's second-generation national identity card', pgs 57-74 in Bennett and Lyon, 2008
- Lyon, D and Bennett, C (2008) 'Playing the ID card: Understanding the significance of identity card systems', introduction to in Bennett and Lyon (2008)

Chatterjee, S (2010) 'We hope Naxals allow census data collection - Q&A: C Chandramouli, registrar general and census commissioner' *Business Standard*, 11 April 2010 <http://www.business-standard.com/>

Economic Times (2010) 'UID has Aadhaar for new name, logo', *Economic Times*, 27 April 2010

Fussell, J (2001) (Prevent Genocide International) 'Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing', presentation to *Seminar Series of the Yale University Genocide Studies Program*, Nov 15, 2001, at <<http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/>>

Greenleaf, G (2010) 'Country Studies B.4 - INDIA' in Korff, D (Ed) *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* European Commission D-G Justice, Freedom and Security, July 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B4_india.pdf>

Greenleaf G (2009a) "Naz Foundation Case expands India's constitutional privacy rights" [2009] ALRS 16; (2009) 100 *Privacy Laws & Business International Newsletter* 24, available at <<http://www.austlii.edu.au/au/journals/ALRS/2009/16.html>>

Greenleaf, G (2009) 'India's new Act creates civil liability for data breaches and criminal offences' (2009) 99 *Privacy Laws & Business International Newsletter* 1-5, June 2009, available at <<http://unsworks.unsw.edu.au/vital/access/manager/Repository/unsworks:8264>>

Greenleaf, G (2008) 'Hong Kong's "smart" ID card: Designed to be out of control', pgs 75-92 in Bennett and Lyon (2008)

Greenleaf, G (2008a) 'Function creep defined but still dangerous in Australia's ID card Bill' *Computer Law & Security Report*, (2008) Vol 24 No 1, 56-66; available on bePress as [2007] UNSWLRS 64

Greenleaf, G (2007) '[Access All Areas: Function Creep Guaranteed in Australia's ID Card Bill \(No. 1\)](#)' (2007) 23 *Computer Law & Security Report* ; [2007] UNSWLRS 11 on Legal Scholarship Network

Greenleaf, G (1987) 'The Australia Card: towards a national surveillance system' *Law Society Journal (NSW)* Vol 25 No9, October 1987; longer version at <<http://austlii.edu.au/itlaw/articles/GGozcard.html>>

Gupta, H (2010) 'Chidambaram has his way as National Intelligence Grid gets PM's okay' *Daily News & Analysis (DNA) website* May 12, 2010 <<http://www.dnaindia.com/dnaprint910.php?newsid=1382016>>

Gupta, R (2010) 'Bourgeois Inspirations' website, section on 'UID Resources' <http://bourgeoisinspirations.wordpress.com/uid-resources/>

Gupta, R (2010a) 'A Gathering Storm - How UID Will Transform India Into A Police State', on *Desicritics.org* website and available at <<http://bourgeoisinspirations.wordpress.com/2010/03/22/how-uid-will-transform-india-into-a-police-state/>>

Gupta, R (2010b) 'Comments On The Draft National Identification Authority of India Bill, 2010' Including 'Some Draft Legislative Safeguards For The Implementation of UID Numbers

(Aadhaar)' (Submissions to UIDAI), July 2010; links to both are at <<http://bourgeoisinspirations.wordpress.com/uid-resources/>>

Jebaraj, P (2010) 'UIDAI draft law by month-end' *The Hindu* 11 May 2010 <<http://beta.thehindu.com/news/national/article426772.ece>>

Kanakia, H, Nadhamuni, S, and Sarma, S (2010) *A UID Numbering Scheme*, UIDAI, May 2010 <http://www.uidai.gov.in/documents/A_UID_Numbering_Scheme.pdf>

Makkar, S and Agarwal, S 'New law to protect individual privacy' *Livemint*, 21 June 2010 at <<http://www.livemint.com/2010/06/20202809/New-law-to-protect-individual.html?atype=tp>>

Mehmood, T 'India's new ID card', pgs 125-127 in Bennett and Lyon (2008)

Mohan, V (2010) 'Census kicks off from April 1' *Times of India* 31 March 2010 <http://timesofindia.indiatimes.com/>

Nilekani, N (transcript of interview) 'We'll use best biometric, storage and search solns'. IGovernment website, 2009 on <www.igovernment.in>

Pillai, G K (2010) 'Home Minister's statement on Census 2011 and NPR' May 10, 2010 <<http://nprindia.blogspot.com/2010/05/home-ministers-statement-on-census-2011.html>>

Ramanathan, U (2010) 'Implications Of Registering, Tracking, Profiling' *The Hindu* 7 April, 2010

Ramanathan, U (2010a) 'Eyeing IDs' *Indian Express*, 1 May 2010 at <<http://www.indianexpress.com/news/eyeing-ids/613701/>>

Torpey, J (2000) *The Invention of the Passport: Surveillance, Citizenship and the State* Cambridge University Press

UIDAI Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission, UIDAI (undated) 2010

UIDAI, 2009 *Creating a unique identity number for every resident in India*, V 1.1, undated, 2009

UIDAI, 2009a *Frequently Asked Questions (FAQs)*, undated 2009

UIDAI, 2009b UIDAI Committee on Biometrics *Biometric Design Standards for UID Applications*, V 1.0, December 2009

UIDAI, 2009c UIDAI DDSVP Committee *Demographic Data Standards and Verification procedure (DDSV) Committee Report*, V1.0, 9 December 2009