

# **UID for Dummies**

Simi Chacko and Pratiksha Khanduri\*

August 2011

Introduction

A. UID: The Basics

B. The Enrolment Process

C. Benefits of UID

D. Concerns: Biometrics, Privacy, Data security, Surveillance

E. UID and Other Databases

F. Similar Initiatives across the World

Endnote

References

Appendix 1: Valid Identification Documents

Appendix 2: ID Systems and Debates across the World

Notes

---

\* The authors are graduate students at Jawaharlal Nehru University (JNU, New Delhi) and the Delhi School of Economics, respectively (contact address: uidfordummies@gmail.com). We thank Reetika Khara and Jean Drèze for their useful inputs and insightful comments.

## INTRODUCTION

The Government of India has embarked upon an ambitious exercise to provide a "unique identification" (or UID) number to every resident of the country. Each number is to be connected with three types of biometric data: iris scans, fingerprints (all ten fingers) and a picture of the face.

UID, it is claimed, will act as a useful identification facility and help the government to root out corruption from social programmes. The project was flagged off with lightening speed in September 2010, when the first residents were "enrolled" under UID in Tembali village, Maharashtra. Since then, no effort has been spared to attract people to enrolment centres.

This urgency in enrolling people has led to a series of misinformed assumptions. Misconceptions range from iris scans being taken for an 'eye test' to fear of ration cards being taken away from those who didn't participate in this 'photography'.<sup>1</sup> Ranjana, the woman who made headlines in September 2010 for being the first person to get a UID number, was in the news again recently after complaining that the number was useless - she had tried to get a travel concession with it on the bus! The conductor bluntly told her to "dump the card in a dustbin".<sup>2</sup> The authorities are not able to clarify these misconceptions because their attention is focused on meeting the enrolment targets.

Meanwhile, the UID project has raised many questions related for instance to privacy, civil liberties, financial costs, and even technical feasibility. Even the Planning Commission is concerned that disquieting "test results" of the UID project have been ignored.<sup>3</sup> Tall claims that UID will enable better management of welfare schemes like NREGA and the PDS have also begun to be questioned. Behind all this, there is a larger question - is there more to UID than meets the eye?

Despite these major concerns, there has been scarce public discussion about key aspects of the UID project. Viewing some of the media coverage that UID has got, it gives a sense of disproportion in the nature of reportage - a bit congratulatory, little depth and few questions asked. This inadequate probing and questioning has led to a lack of understanding within the general population about UID. With that thought, this primer seeks to shed some light on various aspects of this project and answer some frequently asked questions.

The primer relies on official documents (such as the UIDAI's "Strategic Overview", "Handbook for Registrars", "UID and Public Health" paper, etc) as far as the official side of the picture is concerned. This is complemented with other publicly available material, e.g. newspaper articles, reports, interviews, public lectures, websites, etc. As you read on, you will see that on many key aspects of UID, accurate information is not easy to find - we done our best with the material available.

## **A. UID: The Basics**

### **Q. 1. What is UID?**

UID is a “unique identification” number that is to be assigned to every resident of India – one person, one number. This number, aside from being unique for each person, can be verified from his or her fingerprints. It is a little bit like an identity card (or a voter ID) that no-one can lose, steal, forge, or duplicate. What purpose the UID is supposed to serve will be discussed further on.

### **Q. 2. What about UIDAI?**

UIDAI (the Unique Identification Authority of India) is the authority that has been created to issue UID numbers. It was set up in January 2009, by an executive order, *not* a legislative measure such as an Act of Parliament, under the wings of the Planning Commission. The stated goal of the UIDAI is to “issue a unique identification number (UID) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way.”<sup>4</sup> Detailed information about UIDAI is available on the Authority’s website (<http://uidai.gov.in>).

### **Q. 3. Is there a law governing the functioning of UIDAI?**

Not yet. The National Identification Authority of India Bill 2010 (hereafter “NIAI Bill”), tabled recently in the Rajya Sabha, seeks to create a legal framework for UID.<sup>5</sup> If and when the Bill is passed, UIDAI will become a permanent statutory body, renamed National Identification Authority of India (NIAI). The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with NIAI. Meanwhile, the UID process is already in full swing, without any legal framework.

### **Q. 4. On what grounds do we need a UID?**

UID is supposed to act as an all-purpose, fool-proof identification device. This could help, for instance, in preventing “identity fraud” (like impersonation, when someone pretends to be someone else), and in facilitating all processes that require identifying oneself – such as opening a bank account or applying for a passport.

According to the UIDAI’s “Strategy Overview” document, in India “inability to prove one’s identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies.” The document goes on to state: “But till date, there remains no nationally

accepted, verified identity number that both residents and agencies can use with ease and confidence. As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.”<sup>6</sup>

So, the UID project was initiated on the apparent premise that the poor faced great hurdles in accessing benefits and subsidies due to the inability to provide proof of their identity. This problem was always there. It is interesting that it is being “discovered” now, just when a readymade “solution” is in hand. There are, of course, more fundamental reasons why poor people are often excluded from public services and programmes – including the nature of power structures, which tend to be reinforced by projects like UID.

Some healthy scepticism, then, is in order here, especially since there are other views of the real purpose of UID. According to some, for instance, the initial purpose (under the NDA government) was “to wash out the aliens and unauthorized people. But the focus appears to be shifting... Now, it is now being projected as a development-oriented initiative, lest it ruffle any feathers. People would be unwilling to give up their right to privacy.”<sup>7</sup> This is not a human rights activist speaking – it is A.K. Doval, former Intelligence Bureau Chief. And he would know.

It is unlikely that the UPA government would want to be caught on the back foot promoting a surveillance programme initiated by the NDA government. And so begins the consistent effort to manoeuvre and position UID as an unavoidable solution for deep social problems and systemic challenges.

#### **Q. 5. What is “Aadhaar”?**

"Aadhaar" is another name for UID – a sort of "brand name" for the UID project. In Hindi, *aadhaar* means “foundation” – nothing less!

#### **Q. 6. Does getting a UID number entail getting a card?**

It’s a common misconception that getting a UID number means having a legit card with the number. This is not the case. According to some sources, all you get is a UID number on a sheet of paper with personal details. However, various government agencies may or may not, subsequently, issue smart cards using the UID data.<sup>8</sup>

#### **Q. 7. Who is in charge of UIDAI?**

On 2nd July 2009, the Government of India appointed Mr. Nandan Nilekani as Chairman of UIDAI, with the rank and status of a Cabinet Minister, for an initial tenure of five years. Further, the “Prime Minister's Council of UIDAI Authority of India”, set up on 30 July 2009, is to “advise the UIDAI on programme, methodology and implementation to ensure co-ordination between Ministries/Departments, stakeholders and partners”. The first meeting of the Council took place on 12 August 2009”

#### **Q. 8. What is the timeline for this project?**

The timeline for this project has changed a few times. Initially, the target was to start in August 2009. However, this was delayed. The first set of numbers were issued on 29 September 2010, when the UID project was officially flagged off by Prime Minister Manmohan Singh and Congress President Sonia Gandhi in Tembali village, in Maharashtra’s Nandurbar district. The programme plans to provide UID numbers to 600 million people (about half of India’s population) in the next four years.

However, progress has been slow. By July 2011 (almost a full year after the project was launched), about 25 million people – 2 per cent of the population - had been enrolled under UID. Most of the enrolment happened in just three states: Andhra Pradesh, Maharashtra and Karnataka.<sup>9</sup> Having said this, monthly enrolment figures are now growing rapidly.

#### **Q. 9. What is the UID project expected to cost?**

There does not seem to be much clarity on this crucial question. According to some reports, the cost of UID enrolment has risen from Rs 31 per person to somewhere between Rs 450 and Rs 500 per person. By this estimate, this entire exercise will end up costing close to Rs 1,50,000 crores.<sup>10</sup>

Late last year, at a public meeting, Mr. Nilekani stated that the per person enrolment cost is approximately Rs 100.<sup>11</sup> “It costs the Unique Identification Authority of India (UIDAI) Rs.100 to generate each *aadhaar* number, which will help address the challenges of inclusion,” said Nilekani. Even this is an incomplete answer, because several other agencies are also incurring a cost to enrol each person. Because of the way the system of issuing numbers is set up (see below), there is no transparent way to calculate the cost of this project.

According to the Budget documents, Rs 100 crores was approved in 2009-2010 to fund the agency for its first year of existence. This shot up to Rs 1,900 crores in 2010-11. According to columnist Praful Bidwai, the Planning Commission is allocating Rs 35,000-45,000 crores over the next five years - to cover only half the population.

There are also reports that the fund allocation for the first phase is about Rs 3,000 crores. It is a bit worrying that the public can find out about the UID only in phases...

**Q. 10. Is your UID number a proof of citizenship?**

No. Since it is not restricted to Indian citizens, and is meant for all residents of India, the UID number is no proof of citizenship.

**Q. 11. Is it compulsory to enrol under UID?**

“Yes and no” seems to be the answer. The UIDAI claims that UID is a “voluntary facility” – no one is obliged to enrol. However, government agencies are free to make UID compulsory for their own purposes. For instance, nothing prevents the government from requiring NREGA workers to have a UID number in order to get paid. So life without a UID number may end up being quite miserable very soon. As one commentator pointed out, “This is like selling bottled water in a village after poisoning the well, and claiming that people are buying water voluntarily”.<sup>12</sup>

An important point to be noted is that UID’s assurance of casting out “ghost” beneficiaries in programmes like PDS or NREGA can work out only if there is compulsory enrolment, or else both systems of authentication (identity card and Aadhar-based) must coexist - in which case, people with multiple cards may prefer to stay out of the purview of UID.<sup>13</sup>

**Q. 12. What if a person doesn’t have a UID number?**

The UIDAI has been on a Memorandum of Understanding (MoU) signing spree with a range of agencies including banks, state governments and the Life Insurance Corporation of India (LIC) to be “Registrars”, who then may insist that their customers enrol on the UID to receive continued service.

Clause 3 of the draft NIAI Bill, mentioned earlier, declares that “every resident shall be entitled to obtain” a UID number, but nowhere in the Bill is there a clause saying that no agency may refuse services to a person because they do not have such a number. Thus the field is wide open for compulsion.

(A quick aside: Even in the United States, privacy law categorically states that the Federal, State or government agencies cannot deny benefits to individuals who do not possess or refuse to disclose their Social Security Number, unless specifically required by law.<sup>14</sup>)

## **B. The Enrolment Process**

### **Q. 13. Who will issue the UID number?**

The enrolment process is a multi-step process described below. The numbers will be issued through various agencies authorized by the UIDAI across the country, called “Registrars”. The Registrars, in turn, typically sub-contract the enrolment work to “enrolment agencies”.

### **Q. 14. Who is a “Registrar”?**

According to the draft NIAI Bill, “Registrar” means any entity authorized or recognized by the Authority (i.e. UIDAI/NIAI) for the purpose of enrolling individuals under the Act. Potential Registrars include government departments or agencies, public sector undertakings, and other agencies that interact with residents in the regular course of implementing their programmes or activities. Registrars include government, public sector and private sector organizations. For instance, Rural Development Departments (implementing NREGA), Civil Supplies Departments (implementing the PDS), insurance companies such as Life Insurance Corporation, and banks are some of the Registrars currently working on UID enrolment.<sup>15</sup>

So far, the UIDAI has mainly engaged with state governments, central ministries and public sector organizations. The UIDAI has entered into MoUs with state governments, who select the specific departments they would like to appoint as Registrars for the enrolment process.

A Registrar is required to ensure the security and accuracy of data (particularly biometric data) collected from residents. The Registrar must retain the “Proof of Identity/Proof of Address/Consent” for enrolment documents in proper custody for the time period defined in the guidelines issued by UIDAI. They will be held responsible for loss, unauthorized access or misuse of data in their custody. In case of enrolment-related disputes, the Registrar is required to cooperate with the Authority in resolving the matter and provide access to all necessary documents and evidence. As this biometric and demographic data will pass through many hands, the UIDAI will face no action if it fails to protect this sensitive data. If an individual parts with the necessary information, he/she will face penalties. What isn’t clear is how people will know if their data has been breached and privacy violated.

### **Q. 15. What kind of information does one have to provide to get a UID number?**

UIDAI expects all Registrars to collect the following information at the enrolment stage:

Name  
Date of birth  
Gender  
Father's/Husband's/ Guardian's name and UID number (optional for adult residents)  
Mother's/ Wife's/ Guardian's name and UID number (optional for adult residents)  
Introducer's name and UID number (in case of lack of documents)  
Address  
All ten fingerprints, digital photograph and both iris scans

In addition, Registrars may collect other information for their own purposes. For instance, if the Registrar is a bank, it could ask for your telephone number at the time of enrolment.

#### **Q. 16. What are acceptable identification documents for UID enrolment?**

The “Handbook for Registrars”, prepared by the UIDAI, lists documents that can be accepted as valid identity for UID enrolment, such as the ration card, PAN Card, Voter ID etc. (see Appendix 1 for full list).

Those who do not have any of these documents can also apply for a UID number (Aadhaar). In such cases, authorised individuals, who already have an Aadhaar, can introduce residents who don't possess any of the requisite documents and certify their identity. Such persons are called “introducers”.

#### **Q.17. How does enrolment proceed?**

Enrolment is a three-step operation. First, applicants are enrolled by a Registrar or enrolment agency, after recording the information mentioned earlier (name, address, etc.) and collecting the biometrics – photographs, all 10 fingerprints and iris scan. At present, Registrars have been instructed to enrol all persons above the age of five years. Second, the information so gathered is stored in a database called the Central Identities Data Repository (CIDR). Third, this repository is used for de-duplication and, later on, to provide authentication services.

De-duplication will be done by the UIDAI, using the biometrics, to make sure that no-one gets two UID numbers. The UIDAI will also issue the UID number to persons enrolled by Registrars. If any of the personal details (e.g. name and address) recorded at the time of enrolment change, it is the responsibility of the concerned person to alert UIDAI so that the database can be updated – more on this below.



### Other types of identity cards already in use in India

Identity Card	Concerned groups/recipients
PAN Card	Every person with taxable income
Election Photo Identity Card	Indian citizens above 18
Employee Provident Fund Org	Employees in the formal sector
Multi-Purpose National Identity Card	Citizens of India
Rashtriya Swasthya Bima Yojana Card	BPL families
MGNREGA Job Card	Rural residents aged 18 and above
Driving Licence	Citizens aged 18 and above
Passport	Citizens who travel abroad
Ration Card	Families eligible for PDS

#### **Q. 18. Will marginalised persons such as the homeless get a UID number?**

In principle, yes. To refer to the UID website, “the mandate of the Unique Identification Authority of India (UIDAI) includes taking special measures to ensure that Aadhaar is made available to poor and marginalised sections of society, such as street/orphaned children, widows and other disadvantaged women, migrant workers, the homeless, senior citizens, nomadic communities including tribal, and the differently-abled”. However, it is not as simple as it sounds. Recently, an NGO’s homeless shelters were shut down by the Delhi government after it pointed out flaws in UIDAI’s registration of the homeless. The NGO, Indo Global Social Service Society (IGSSS), stopped the enrolment process of the homeless after they realized that there was no clarity on what the NGO’s liability would be. Not only were the homeless being registered at the NGO’s address, their volunteers were asked to be the “introducers”. After one of its employees got questioned by the police for the death of a homeless person because a survey slip was found in the deceased’s pocket, the NGO decided to seek detailed information about the programme from the government, but their queries were not answered.<sup>16</sup> This story is also a useful reminder of the dangers of initiating UID enrolment without a clear legal framework.

#### **C. Benefits of UID**

#### **Q. 19. What are the claimed benefits of enrolling under UID?**

UID is supposed to act as a general identification facility: “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.”<sup>17</sup> How useful this “facility” is (and whether it is itself hassle-free) remains to be seen. Aside from this, it is claimed that the UID project is a powerful tool to fight corruption in welfare programmes, enhance inclusiveness in government schemes, and so on. Tall claims have been made, e.g., “the project possesses the power to eliminate financial exclusion, enhance accessibility, and uplift living standards for the majority poor.”<sup>18</sup> Some of the specific areas where the benefits of UID are supposed to flow are the National Rural Employment Guarantee Act (NREGA), the Public Distribution System (PDS), public health, financial inclusion, etc. How this is supposed to happen is explained in a series of concept notes posted on the UIDAI website. Three of these concept notes are critically discussed below. The intention is not to say that UID is necessarily useless, but to debunk exaggerated claims and point out that the real benefits are yet to be clearly identified.

Before we proceed, it is worth noting that the UIDAI’s concern with welfare schemes like NREGA and the PDS is not entirely disinterested. There is a catch: imposing UID on welfare schemes is a way of promoting UID enrolment. As one analyst (who is “working on the project but did not want to be identified”) put it, “the foremost priority for UIDAI right now is to get people hooked on to using its applications”.<sup>19</sup> Since NREGA and the PDS are some of the biggest welfare schemes, covering most of the rural population, it is no wonder that they were identified early on as potential channels of mass enrolment. Sometimes, it looks like UIDAI needs NREGA and the PDS more than the other way round.

#### *UID and NREGA: Claims and clarifications\**

Unsuspecting readers of the UIDAI’s concept note on “UID and NREGA” may be bowled over by the power of Aadhaar.<sup>20</sup> However, a closer look suggests that scepticism is in order.

**Muddled thinking:** “Once each citizen in a job card needs to provide his UID before claiming employment, the potential for ghost or fictitious beneficiaries is eliminated.” Elimination of ghost beneficiaries would be an important contribution, but as the same sentence makes clear, it requires compulsory and universal enrolment. Yet public statements convey that UID enrolment will be voluntary.

---

\* This section and the next draw on Reetika Khera, “Not all that unique”, *Hindustan Times*, 30 August 2010; see also Khera (2011).

**Poorly informed:** "In many areas the wages continue to be paid in the form of cash." In fact, the transition to bank payments is largely complete (83% of NREGA job card holders have an account). Tamil Nadu is the only "area" where wages continue to be paid in cash (retained for the sake of speed).<sup>21</sup> The introduction of payments through bank or post office accounts has made corruption quite difficult, but three ways of siphoning off money remain - extortion, collusion and fraud. Extortion means that when "inflated" wages are withdrawn by labourers from their account, the middleman turns extortionist and takes a share. Collusion occurs when the labourer and the middleman agree to share the inflated wages that are credited to the labourer's account. Fraud means that middlemen open and operate accounts on behalf of labourers, and pay them cash. Biometric-enabled UID to authenticate identity can only help to prevent "fraud", but is of little use in preventing collusion or extortion.

**Financial inclusion:** Payment of NREGA wages through banks and post offices have been made mandatory since 2008. Transition from cash to bank or post-office payments is presently complete to a large extent. In fact, over 9 crore NREGA accounts (covering 83% of NREGA job card holders) were opened by 2009-10, without UID in the picture.

**What about corruption in material purchase:** UID can address only some of the wage-related fraud in NREGA; it can do little about material-related corruption, a serious concern in recent years.<sup>22</sup>

**Theft from beneficiaries:** Benefits of the UID project are contingent on beneficiary verification at the point of service. Therefore delivery of service will depend on functional biometric equipment. This creates the following issues: (1) Every single point of service must be equipped with a biometric reader e.g., all NREGA worksites – there are about 600,000 and the simplest biometric readers cost at least Rs 2,000 each. (2) Damage of biometric readers, due to normal wear and tear or other causes (including possible sabotage), will disrupt service delivery. Any contingency measures that bypass biometric authentication will be vulnerable to fraud. (3) Corruption is rampant and requires comprehensive safeguards; a static single-point mechanism is likely to be unreliable in the medium to long-term.

**Disruptive potential:** Last but not least, UID could easily disrupt NREGA's fragile processes. The UIDAI plans to involve "service providers" who will enrol individuals for UID. Later, they will be involved in authentication of workers at worksites. The result of such changes will be drastic for NREGA. Payments will come to a halt if workers are still waiting for their Aadhar number. And "service providers" are all set to invade NREGA, outside the framework of the Act, without any safeguards.

Because of this potentially disruptive role of UID in NREGA, nearly 200 scholars and activists signed and circulated a petition called “Keep UID Out of NREGA!” in December 2010.<sup>23</sup> The concerns raised in that petition are yet to be answered.

### *Will UID Fix the PDS?*

Similar reservations apply to the UIDAI’s concept note on “UID and PDS System”.<sup>24</sup> Again, tall claims are made without an adequate understanding of how the PDS works.

**Dealing with exclusion from social benefits:** The UIDAI claims that the project can help to deal with the fact that many poor people do not benefit from government welfare schemes such as the PDS. The reason behind this, according to the UIDAI, is that people do not have an identity. However, in the case of the PDS, the two main reasons for the poor being excluded are that (a) the government is willing to provide subsidized food to too few people (“low coverage”) and (b) there is “misclassification” of households. This means that because the government’s criteria for identifying the poor, and the implementation of these guidelines, are faulty, many poor families are excluded. UID can do nothing about these two problems.

**Bogus cards and de-duplication:** One of the main claims is that UID will eliminate “bogus” cards. The UIDAI seems to be unable to distinguish between the various types of bogus cards: (a) “ghost” cards, i e, where cards exist in the names of non-existent or deceased persons; (b) “duplicates” where one person or household, entitled to one card, manages to get more through unfair means; and (c) “misclassified” cards, when *ineligible* households or persons claim benefits (or, inclusion errors). The UID can help deal with the first two, but not the third type of bogus cards (on that see “classification errors” below).

The next question then is, how large is the problem of “ghost” or “duplicate” cards. That question is not easy to answer. It is not clear how large the problem of duplicate or bogus BPL cards actually is. If the recent example of Tamil Nadu weeding out bogus cards is any evidence, then it is only 2% (Planning Commission, 2004). Chhattisgarh tried to achieve de-duplication by computerizing the database of ration card holders and distributing ration cards with holograms, without relying on UID. Eight per cent of cards were found to be “duplicate”.

Further, the elimination of ghost and duplicate cards requires that UID enrolment be compulsory and universal. This is best explained by Nandan Nilekani himself (in an interview to Outlook Business in October 2010): “You can’t make it mandatory in the first instance. Let’s say a particular state decides to issue fresh ration cards from 1 May 2011.

Now, they may decide to have Aadhaar numbers on all these cards. For some time, in parallel there will be the earlier cardholders who will not have Aadhaar. We can't completely eliminate duplication. But over time, as Aadhaar numbers in ration cards become nearly universal, they can then say 'from now onwards, only Aadhaar-based ration cards will be accepted'. At which point, duplication will cease to exist."

**Classification errors:** One of the major problems with the existing, targeted PDS is that of classification errors: many poor families are not identified as poor ("exclusion errors") and better-off families often get the benefits ("inclusion errors"). According to Drèze and Khera (2010), nearly half of the poorest 20 percent did not have BPL cards in 2004-5. UID will not be able to correct this as it will only verify if the beneficiary exists and is unique. Consequently, the UID number won't be able to solve the problem of misclassification.

**"Last mile" problem:** Another common problem is that PDS dealers "short-change" their customers: they give them less than their entitlement, and make them "sign" for the full amount. Again, UID will be of little help here. If customers can be duped into signing (or giving their thumbprint) for more than what they are given, they can surely be convinced to give their UID number for the same purpose.

**Upstream Leakages:** A large part of the PDS leakages happen before the foodgrains reach the PDS dealer. For example, much of PDS grain used to be diverted between government godowns and the village ration shop. The UID project is not designed to deal with upstream leakages in the distribution and delivery systems.

**Portability:** The UIDAI also makes a claim of "portability of benefits", i e, that with a UID, beneficiaries can claim their benefits wherever they are. A PDS that allows beneficiaries to draw their rations from anywhere in the country would indeed be a desirable improvement over the present system. The portability argument is perhaps the most enticing aspect of the UID programme as far as the PDS is concerned. However, this too is not very well thought through. Though the UID is portable, benefits may not be, because the latter present operational issues that cannot be solved by the UID.

A more plausible contribution of UID to "PDS reform" is that it would facilitate the transition to cash transfers (instead of food entitlements), advocated by many economic advisers and policy-makers. This move, however, is itself fraught with dangers.<sup>25</sup>

### *UID and Public Health*

A study by Oxford University holds that in India, more than a million people die every year due to lack of adequate healthcare. Also, 700 million people have no access to specialist care, as 80 per cent of the specialists live in urban areas.<sup>26</sup>

Against this background, the UIDAI shrewdly identified public health as a “killer application” (sic) for UID. As the UIDAI’s concept note on “UID and Public Health” states:

“Existing data bases would probably still leave a large percentage of the population uncovered. Therefore every citizen must have a strong incentive or a “killer application” to go and get herself a UID, which one could think of as a demand side pull. The demand and pull for this needs to be created *de novo* or fostered on existing platforms by the respective ministries. Helping various ministries visualise key applications that leverage existing government entitlement schemes such as the NREGA and PDS will (1) get their buy-in into the project (2) help them roll out mechanisms that generate the demand pull and (3) can inform a flexible and future-proof design for the UID database. It will also build excitement and material support from the ministries for the UID project even as it gets off the ground.”<sup>27</sup>

The game plan could hardly be more explicit.

Mohan Rao, a professor at the Centre of Social Medicine and Community Health (JNU, New Delhi) articulated a scathing critique of UIDAI’s lofty claims about uplifting the public health situation in the country.<sup>28</sup>

“The UID working paper on public health would have us believe that these changes occurred because of a lack of ‘demand’ for healthcare, as it sets out what it calls a ‘killer application’ to provide citizens an incentive to obtain a UID card in order to meet health needs. This unfortunate language apart, the fact that we have not built a health system is hardly fortuitous. It is true that we do not have good quality health data or indeed even vital statistics; it is true that this should come from integrated routine health system and not ad-hoc surveys.”

He asserts that UID is not devised to deal with the public health challenges of our country. “On the contrary, given that many diseases continue to bear a stigma in this country, the UID scheme has the unique potential of increasing stigma by breaching the anonymity of health data collected. It thus violates the heart of the medical encounter, namely confidentiality. By making this information potentially available to employers and insurance companies, the scheme bodes further gross violations of health rights.”

Referring to the NGO reports about the Delhi government’s “Mission Convergence” scheme, under which biometric health insurance cards were issued to slum dwellers by which they could avail free treatment, Rao holds that there have been a lot of complaints about

malfunctioning fingerprint readers, despite multiple swipes. He advises the Health Ministry to hold back on their support for UID until a conclusive study of the costs and risks of this project is undertaken.

#### **D. Concerns: Biometrics, Privacy, Data security, Surveillance**

##### **Q. 20. What are biometrics?**

Biometrics is the science of identifying persons based on their physical (e.g. fingerprints) or behavioural (e.g. voice) traits. It builds on the fact that individuals are physically and behaviourally unique in many ways. Technically, biometrics has been defined by experts as “the automated recognition of individuals based on their behavioural and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges).”<sup>29</sup>

Post “9/11”, many countries have overhauled their surveillance mechanisms through legislations and technological upgrades, and subjected the public to scrutiny. When this revamp began, the use of biometrics came to be seen as inevitable. Fierce debates emerged, as opponents have raised strong arguments against intensive monitoring, profiling and invasion of privacy. Though some of these objections stem from exaggerated fears of being victimised by government agencies wielding excessive power, others are not unjustified.

##### **Q. 21. What are the technological concerns that face UID?**

Many concerns have been expressed about the technological feasibility, reliability and safety of the UID project. Here are some.

A recent NASSCOM document, prepared by Dr. Kamlesh Bajaj, points out that since the UID database has to be accessible over networks in real time, it involves major operational and security risks - as with any such applications.<sup>30</sup> If networks fail or become unavailable, the entire identification system may collapse. Biometric and other data may become a target for hackers and other malicious entities. “Such a system is also prone to functional creep (secondary uses) and insider abuse. There is also a significant risk of transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection”.

Another concern is the reliability of biometrics. For instance, since iris development does not take place till the age of 7 years and children do not have sharp patterns of fingerprints till they are 15, giving children UID numbers is a huge challenge. Also, worn-out fingers of farmers and manual labourers will be difficult to scan, and an iris scan can't be done on people with corneal blindness or corneal scars. Some experts also argue that manufacturers have not been able to put into practice a fingerprint system that can effectively distinguish human fingers and artificial fingers of silicon, rubber, acrylic, paint, etc.<sup>31</sup>

Aside from the costs of employing such a system, inclusive of not just the financial expenditure, but also of the time and effort it takes to enrol individuals and collect their biometric data, 100% reliability in authentication can never be guaranteed. A large proportion of biometric trials have been conducted in the “frequent traveller” setting, among volunteers who are primarily white male professionals in the 20-55 age groups.<sup>32</sup> Diverse conditions will throw up more challenges to such a system.

**Q. 22. Does UIDAI currently function under the purview of a law?**

Ironically enough, UIDAI has been on an enrolling spree since September 2010 without a law sanctioned by the Parliament. However, as we saw, the proposed NIAI Bill seeks to establish the National Identification Authority of India (NIAI) as a statutory authority and lay down rules, processes and safeguards concerning Aadhaar. The NIAI would consist of a chairperson and two part-time members. The bill also authorizes the creation of an Identity Review Committee, designed to monitor usage patterns of UID numbers.

The Bill states the date of the Act coming into force as being subject to its notification by the Central Government in the gazette once the Parliament passes it. Now what is problematic here is that the collection of biometric and personal data and issuing of UID cannot and do not have any statutory sanction until the bill is passed by Parliament. Demographic and biometric information to be recorded have been left to regulations, empowering the NIAI to collect additional information without prior approval from Parliament.

Additionally, Clause 3(1) of the bill does not make it compulsory for individuals to enrol, but, as mentioned before, nothing prevents service providers or government agencies from positioning UID as a pre-requisite for availing services.



## Biometrics: Reliable or Fallible?

Over the years, biometrics are being used more and more for a wide variety of purposes, such as to “recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders.”

Here’s why biometric systems have a shaky base:

- Variation within persons: Biometric information may be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, socio-cultural aspects of the situation in which the presentation occurs, changes in human interface with the system, etc.
- Sensors: “Sensor age and calibration, how well the interface at any given time mitigates extraneous factors, and the sensitivity of sensor performance to variation in the ambient environment (such as light levels) all can play a role.”
- Feature extraction and matching algorithms: “Biometric characteristics cannot be directly compared but require stable and distinctive ‘features’ to first be extracted from sensor outputs”. For example, every finger of an individual will generate a different image due to external factors such as dirt, moisture, etc. Therefore these multiple impressions from one finger can be matched by good algorithms to the correct finger source.
- Data integrity: “Information may be degraded through legitimate data manipulation or transformation or degraded and/or corrupted owing to security breaches, mismanagement, inappropriate compression, or some other means.”

Also, social, cultural and legal factors come to have a bearing on such a system’s acceptance by its users, its performance, or whether a system like this should be adopted in the first place. Such factors need to be unequivocally taken into consideration while designing the system. That is to say, the effectiveness and accuracy of the system is contingent on user behaviour which in turn is shaped by the larger social, cultural and legal context.

“When used in contexts where individuals are claiming enrolment or entitlement to a benefit, biometric systems could disenfranchise people who are unable to participate for physical, social, or cultural reasons. For these reasons, the use of biometrics— especially in applications driven by public policy, where the affected population may have little alternative to participation—merits careful oversight and public discussion to anticipate and minimize detrimental societal and individual effects and to avoid violating privacy and due process rights.” (p. 10)

Another disquieting aspect of biometric systems is the potential for misuse of power. Many experts have suggested that such fears must be addressed with all seriousness.

Although biometric systems have penetrated many areas, like identifying terrorists, criminals, personalization of social services, better control of access to financial accounts, etc, yet, a number of unsettled questions remain regarding the effectiveness and management of systems for biometric recognition, as well as the appropriateness and societal impact of their use. It looks set to expand into more areas but the intrinsic concerns of such a system have clearly not been adequately addressed. Not even close.

**Source:** *Biometric Recognition: Challenges and Opportunities*, Joseph N. Pato and Lynette I. Millett (eds.); Whither Biometrics Committee, National Research Council, 2010.

Though the information gathered by the NIAI may be shared with other agencies with the consent of the UID number holder, in this bill, the safeguards for protection of privacy of individuals are weak. Under Clause 33 (b), the NIAI is required to disclose identity information in the interest of national security, if so directed by an authorised officer of the rank of Joint Secretary or above in the central government. The safeguard for protection of privacy differ from the Supreme Court guidelines on telephone tapping; these permit phone tapping under threat of “public emergency” for a period of six months, while information gathered by UID can be shared in the interest of national security, offering no review mechanism.

This leaves space for profiling and surveillance of individuals by intelligence agencies, as nothing in the bill prevents them from using the UID to “link” various databases (such as telephone records, air travel records, etc.). This kind of a system could lead to persecution of innocent individuals who may get tagged falsely as potential threats.

As far as “Offences and Penalties” are concerned in this bill, it holds that no court shall acknowledge any offence except on a complaint made by the NIAI. This effectively exempts NIAI of any public accountability. This heavy concentration of power in a single authority is alarming and raises grave doubts about just how transparent this system really is.

### **Q. 23. How does UID impact privacy concerns in India?**

Internationally, there is growing concern about privacy and its protection. In India, however, paying lip service to this issue once in a while is as good as it gets. (Although in May 2000, the Indian government passed the Information Technology Act, a set of regulations meant to provide a comprehensive regulatory environment for electronic commerce).

Despite all assurances about protection of sensitive information on mass scale, it must be acknowledged that any database that stocks up such personal information brings with it the risk of misuse by various agencies be it public or private, impinging on an individual’s privacy. Even UIDAI chief Nandan Nilekani has conceded, on record, that the country needed well-defined privacy laws to prevent any malicious use of data. Regarding the possibility of data being misused, he said that the only service provided by the UIDAI was that of authentication.

In the NIAI Bill, there are sketchy descriptions of offences like “intentionally” accessing the UID database and damaging, stealing, altering or disrupting the data. But it provides no means for a person whose data is stored to know that such an offence has been committed;

and it does not allow prosecution to be launched except on a complaint made by the authority or someone authorised by it.

So, given the lack of privacy laws in India, “convergence” of the UID database with other systems could spell a lot of trouble.

A related danger is “tracking”. This stands to alter the relationship between the state and the citizen. With the integration of databases, the state would have enormous power to track people’s movements and communications, or to profile them.

#### **Q. 24. Is there a redressal mechanism?**

It is unclear as to how errors and inaccuracies in the UID database will be corrected as they emerge. Under the proposed NIAI Bill, if someone finds that his/her “identity information” is wrong, he/she is supposed to “request the Authority” to correct it, upon which the Authority “may, if it is satisfied, make such alteration as may be required”. So although there is a legal compulsion to alert the Authority, there’s no *right* to correction.<sup>33</sup>

### **E. UID and Other Databases**

#### **Q. 25. What is NATGRID?**

In a lecture he gave at the 22<sup>nd</sup> Intelligence Bureau Centenary Endowment in December 2009, Home Minister P. Chidambaram announced that the central government had decided to create a National Intelligence Grid (NATGRID). “Under Natgrid, twenty-one sets of databases will be networked to achieve quick seamless and secure access to desired information for intelligence and enforcement agencies,” he said.<sup>34</sup> Under this, the UID number of each individual will become the link between the different databases. These databases would be integrated with information available not just with government agencies and public sector, but also private organizations such as banks, insurance companies, stock exchanges, airlines, railways, telecom service providers, chemical vendors, etc. This would give security agencies the power to access sensitive personal information such as bank account details, market transactions, websites visited, credit card transactions etc.

In the 2011-2012 budget, NATGRID got an allocation of Rs. 41 crores. With an estimated overall budget of Rs 2,800 crores and a staff of 300, NATGRID is supposed to be a “world-

class” measure for combating terrorism and dealing with internal security threats. NATGRID is headed by Captain Raghu Raman, former Chief of Mahindra Special Services Group.<sup>35</sup>

Telecom and internet service providers will be obligated by regulations to link up their databases with NATGRID: “The databases so far identified for being linked in the grid include those of rail and air travel, phone calls, bank accounts, credit card transactions, passport and visa records, PAN cards, land and property records, automobile ownership and driving licences.” In India, a citizen has virtually no legal protection against government surveillance. In a petition filed by People’s Union for Civil Liberties (PUCL) in 1996, the Supreme Court ruled against arbitrary surveillance. This was overturned by Parliament with the passage of the Information Technology (Amendment) Act 2008. No political party raised any objections when the government passed this Act, which removed certain safeguards against surveillance.

In a case pertaining to invasion of privacy, pending before the Delhi High Court, the Court observed: “We have no clear definition of what is meant by ‘invasion of privacy’ within the RTI Act.”

Then in February 2010, the Cabinet Committee on Security expressed its reservations to the Home Ministry about protection of individuals’ privacy within NATGRID and its zealous goals, and held up its development till the ministry prepared a detailed report on “inbuilt safety mechanism.”<sup>36</sup>

That wasn’t the only hiccup. Even Finance Minister Pranab Mukherjee adopted a cautious tone in a hand-written note addressed to NATGRID’s CEO, Raghu Raman. "Intrusion into privacy of the bank depositors is just not acceptable as it will discredit the banking system and the people will start using other modes for securing their funds and carry on transactions," said Mukherjee.<sup>37</sup> This was a reaction to Raman’s efforts at giving directives to the Reserve Bank of India (RBI) to allow his organisation access to individual savings accounts through the district magistrates to identify the “terror money trail”.

#### **Q. 26. What is Crime and Criminal Tracking Network and Systems (CCTNS)?**

The Crime and Criminal Tracking Network and Systems (CCTNS), on the other hand, with an outlay of Rs 2,000 crores, aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at the police station level through interlinking CCTNS with UID. It would facilitate exchange of data on criminals. Around 20,000 police stations, courts, fingerprint bureaus, forensic laboratories etc., will be linked on a national databank, thereby helping people to lodge and track complaints on line. Linking of

UID with such e-governance projects will lead to consolidation of data and greater profiling by the state.

**Q. 27. What is the National Population Register (NPR) and how is it linked to UID?**

The arduous task of providing over a billion people with a UID number also overlaps with the mandatory Census of 2011, which will ultimately lead to the establishment of the National Population Register (NPR). The NPR project has not been initiated under the Census Act, 1948. It is being carried out under the Citizenship Act of 1955 (after an amendment was made) and the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003.

After a cabinet meeting in March 2010, chaired by Prime Minister Manmohan Singh, the creation of NPR was approved. “The project would cover an estimated population of 1.2 billion and the total cost of the scheme is Rs 3,539.24 crores,” Information and Broadcasting Minister Ambika Soni told reporters.<sup>38</sup> She said the creation of a digital database with identity details of all individuals along with their photographs and finger biometrics “will result in the creation of a biometrics based identity system in the country... will enhance the efficacy of providing services to the residents under government schemes and programmes, improve the security scenario and check identity frauds in the country”.

Data for the NPR will be collected along with the house listing and housing census which started in April 2010, and was supposed to be completed by September 2010. The NPR database, on being finalized, is to be sent to the UIDAI for biometric de-duplication and allocation of a UID number. “This number will be added to the NPR database,” Soni said.

Little is known about how the government plans to integrate UID with NPR. In the village of Tembali, both were meant to work together in capturing biometrics. The Census Office (also known as the Registrar General of India) has been given the authority to collect the biometric data through an Act of Parliament. But the information recorded by the private enrolment agency working for UIDAI is different from the details captured by the census enumerators. Unique identity numbers were meant to be issued by the agency based on the information recorded for NPR. This meant that while every Indian resident would have an NPR card and a UID number, the enrolment was meant to be carried out by the Census office<sup>39</sup>.

But for now it looks like the private registrars working on behalf of UIDAI do not have access to the digitised NPR information and have started the collection process again. In a recent report, it was found that in Sahada, a tehsil in Nandurbar (Maharashtra), the residents were being enrolled again even though they were the first recipients of UID cards in the

country last September. Tera Software Limited, the registrar in Sahada, has been collecting information which doesn't match with the details collected by the census office. While the census captured demographic data such as name, address, educational qualifications etc, the UID enrolment form has been asking residents to fill up information such as voter card number, PAN number, LPG connection number, etc.

Recently, UIDAI put forward a request to the government for an additional Rs. 15,000 crores to enrol the population by capturing the biometric data by using its own agents. This means that if both Census and UIDAI carry out their own enrolments, it would cost the government an additional Rs 10,000 to 40,000 crores.<sup>40</sup> Also, while the UID is doling out incentives for people to register, NPR has no such plans. Because of this, states such as Rajasthan, Madhya Pradesh and Gujarat have opted out of NPR. While UIDAI has relied on 209 registrars as part of its "outsourced service oriented" infrastructure, concerns have been raised about private enrolment agencies handling personal data such as bank account details.

The risk of misuse gets greater as some of the enrolment agencies such as Alankit Assignments, Alankit Finsec and Alankit Lifecare have a stake in the healthcare and insurance sectors. Some private enrolment agencies such as Tera Software have been found sub-contracting the work to other firms without government approval.<sup>41</sup> A group of central public sector firms and the Department of Information Technology are responsible for capturing biometric data for NPR. Concerns were raised by the Standing Finance Committee of the Parliament for the Ministry of Planning about UIDAI collecting biometric data without any legal approval.

There are critical arguments against such linking of data. Says law researcher and rights activist Usha Ramanathan: "There is an express provision regarding 'confidentiality' in the Census Act, which is not merely missing in the Citizenship Act and Rules but there is an express objective of making the information available to the UIDAI for instance, which marks an important distinction between the two processes. Section 15 of the Census Act categorically makes the information that we give to the census agency 'not open to inspection nor admissible in evidence'. The Census Act enables the collection of information so that the state has a profile of the population; it is expressly not to profile the individual."<sup>42</sup>

She continues, "The information gathered in the house-to-house survey, and the biometrics collected during the exercise, will be fed into the UID database. This will provide the bridge between the 'silos' of data that are already in existence, and which the NPR will also bring into being."

And now to briefly turn to UK's experience when the proposal of initiating a National ID system was in consideration. It saw a multitude of arguments from civil society activists and the media about the issue. "The government wants to reassure us. It says it's trustworthy; it says there's a lot of scattered data out there about us anyway - surely it's just common sense to link it up? Yet security experts know that the linking and aggregation of detailed personal information on this gigantic scale will be unstable and dangerous to everyone, because of the depth of what it reveals, because of its secrecy and because it will present a vulnerable target for electronic attack, whether by hostile governments, by international terrorism, or by your spiteful colleague," says Christina Zaba, a journalist and activist.<sup>43</sup>

**Q. 28. How is UID related to NATGRID, CCTNS, NPR and other databases?**

The UID number will be fed into a database to be shared with NATGRID, which includes 11 security and intelligence agencies (Intelligence Bureau, Research and Analysis Wing, CBI, Central Boards of Excise and Direct Taxes, etc). This kind of cross agency interlinking will enable them "to detect patterns, trace sources for monies and support, track travellers, and identify those who must be watched, investigated, disabled and neutralized".<sup>44</sup>

"There are presently various pieces of information available separately, and held in discrete 'silos'. We give information to a range of agencies; as much as is necessary for them to do their job...The ease with which technology has whittled down the notion of the private has to be contained, not expanded. The UID, in contrast, will act as a bridge between these silos of information, and it will take the control away from the individual about what information we want to share, and with whom," says Usha Ramanathan.<sup>45</sup>

**Q. 29. Is there a role for private sector firms in the UID project?**

There's a good reason why the UID project is getting a unanimous thumbs up from the corporate sector. Initial estimates suggest that the project will create 1,00,000 new jobs in the country, and business opportunities worth Rs 6,500 crores in the first phase.<sup>46</sup>

The UID project, built on the PPP model, is a complicated system that depends on complex technology. Aside from issuing UID numbers, the UIDAI is expected to act as a regulatory authority, manage a Central Identities Data Repository (CIDR), update resident information and authenticate the identity of the residents as required.

UIDAI has awarded four consortia (Accenture, Mahindra Satyam, Morpho and L1-Identity Solutions) to implement core biometric identification systems in support of the Aadhaar programme. Essentially these four agencies would design, supply, install, commission, maintain and support the biometric identification subsystem. They would also be involved in

the development of a software development kit (SDK) for client enrolment stations, the verification server, manual adjudication and monitoring functions of the UID application.<sup>47</sup>

As far as Accenture is concerned, the terms of its initial contract will run up to two years or until 200 million enrolments have been registered (whichever comes first). Along with Accenture, the team includes Daon, a leading global provider of biometric technologies, and MindTree, a Bangalore-based global IT company that delivers innovative technology solutions. L-1 Identity Solutions is a large American defense contractor in Connecticut. It was formed in August 2006 from a merger of Viisage Technology and Identix Incorporated. It specializes in selling face recognition systems, electronic passports such as Fly Clear, and other biometric technology to governments such as the United States and Saudi Arabia. It also licenses technology to other companies internationally, including China.

Also, the contracts for purchase of biometric devices have been bagged by Tata Consultancy Services (TCS), HCL Info Systems Ltd, Base Systems Pvt Ltd, 4G Identity Solutions Pvt Ltd, e-Smart Systems Pvt Ltd.

Private players are set to reap the benefits. “We considered 2009 as a launch year for the expo entirely focused on homeland security and we saw over 130 companies from 15 countries participate. Next year we expect larger participation, especially from the US and European countries including France and Russia,” Mehul Thakkar, marketing manager of INDESEC, said.

### **Q. 30. More than meets the eye?**

With regard to L1 Identity Solutions, it is interesting that former Central Intelligence Agency (CIA) and other American defense organisations’ officers are now working in the capacity of directors and other positions in the top management of the company. While that is not exactly illegal, it has overtones of inappropriateness. George Tenet, former director, CIA, is on the board of directors of L1 Identity Solutions, among other similar organizations, and has been accused, not without reason, of profiting from the involvement of such companies in the Iraq war.<sup>48</sup> Also Safran, a French company, acquired L-1 Identity Solutions following the sale of L-1's intelligence services businesses to BAE Systems. After giving effect to the BAE Systems transaction, L-1 will consist of Secure Credentialing Solutions, Biometric and Enterprise Access Solutions and Enrolment Services.

In the United States, L-1 not only manages the state driver’s license business but is also engaged in the production of all passports, provides identification documents for the



Department of Defense and has contracts with nearly every intelligence agency in the government. L-1 was rejected by US government agencies on grounds of low quality of its biometric cards. In June 2010, a support contract unit of L-3 Communications Corp said it was de-listed from providing service to any federal agencies in the US. The support contract unit was providing aircraft maintenance and logistic support to the US Air Force. The unit allegedly used government computer networks to collect data to promote its own business. In September 2010, the company received US\$ 24 million for the project from the UIDAI. The company has already shipped some units of the Agile TP fingerprint slap devices and mobile iris cameras. In a Forward Looking Statement the company said it hopes to complete the remainder of the shipment by March 2011.<sup>49</sup>

Mark Lerner, who is with the Constitutional Alliance (an American non-profit educational organisation) and is also the author of the book *Your Body is Your ID*, says: “To a large extent it is fair to say that your personal information is L-1’s information. L-1 is the same company that thinks our political party affiliation should be on our driver’s license along with our race.” Commenting on L-1’s acquisition by Safran, he continues: “Just think about how happy you can feel now knowing that your personal information including your social security number and biometric information (fingerprints, iris scans and digital facial images) may soon be available to a French company. The federal government must sign off on the deal before the deal can be sealed. All this brings us back to the topic of the revolving door that exists between government and corporations.”<sup>50</sup>

The prospect of such companies having a deep reach into the massive sensitive UID database would make any person weary.

**Q. 31. Are there any other business interests in UID we should be concerned about?**

Yes. For instance, there is a vast potential for UID applications in the field of marketing. UID seems set to facilitate charting of consumption patterns to an integrated pan India database which “would work towards promoting India as an accessible market place for banking, financial and other institutions”.<sup>51</sup> This is possibly going to alter the idea of citizenship drastically in the end.

Addressing the Nielsen Company's “Consumer 360” event in New Delhi on 25 November 2010, UIDAI Chairman Nandan Nilekani said that over a third of India's 1.1 billion “consumers” had been largely overlooked in areas such as banking and social services.<sup>52</sup>

“The (unique identification) number will create a much more open marketplace, where hundreds of millions of people who were shut out of services will now be able to access them,” he told business leaders, adding that the poor find it difficult to reach the market.

"Their anonymity limits agencies from providing them services that are remotely available, and that could be accessed through a mobile phone," he said.

There is a definite move in the industry to co-opt the public on the use of sensor technology and how it can radicalize everyday life. According to Infosys's chief executive officer S. Gopalakrishnan, sensor technologies integrated with IT networks, cloud computing, and the mobile internet "will drive investment, and change how companies automate business processes in the future".<sup>53</sup> Integrated sensor technologies are attuned to identifying a customer entering a store and offer her new products and customized discounts based on her prior buying behaviour, he adds.

The use of biometrics in consumer ID applications worldwide are projected to grow at a Compound Annual Growth Rate (CAGR) of around 27% between 2010 and 2012.<sup>54</sup> With advancements in sensor technology and algorithms, biometrics seem to have become a choice for the financial services industry as well.

## **F. Similar Initiatives across the World**

### **Q. 32. How have other countries approached such projects?**

Debates about systems of national identification have been taking place worldwide for a long time, but with a growing intensity in the last few years. Technological progress and the current socio-political scenario have led to growing support for complex ID systems from governments and particular sections of the population. Below is a brief description of similar projects across the world (for country-specific details, see Appendix 2).

Some of the most prolific examples of National ID programmes and their subsequent outcomes can be seen in Australia, UK and the US. Australia witnessed perhaps the fiercest opposition to national ID cards. In 1985, there was a proposal to introduce these cards (mostly for curbing tax evasion) but due to severe backlash from activists and citizens, backed by strong media support, it was withdrawn in 1987.

The Real ID Act passed by the US in 2005 has also been opposed by many states on grounds of privacy and threat to data security. As a compromise, the Obama administration, in 2009, introduced Pass ID in the Congress. The Pass ID Act sets strong security standards for identification cards and driver's licenses. However, it does not collect personal information of individuals and store it in a centralized database, accessible by any state authority, as the UID project does.

After many deliberations and public debates, the “UK National Identity Card Scheme” was scrapped in 2011 by the Conservative-Lib Dem Coalition. Some of the primary reasons cited were the cost of implementing the scheme (£4.5bn) and the infringement of civil liberties. Among European nations, many have ID cards, voluntary or mandatory. An interesting case is that of Germany. Starting in November 2010, German ID cards were incorporated with RFID chips containing personally identifiable information including a biometric photo and, if desired, two fingerprints. After a group hacked the new national ID system, live on TV, Germany's Federal Office for Information Security acknowledged that the card's PIN can be cracked using trojan malware, similar to keylogging software.

Some Middle Eastern countries are planning to issue “smart” ID cards, with Oman taking the lead. The ID card in Oman stores fingerprints, but information on the card is not given to all government agencies nor the private sector.

In Asia, one country worth mentioning is Malaysia, which has made a successful transition to a smart card containing personal information including health details and driving licenses. Taiwan's attempts to introduce a national ID card with fingerprints met with severe opposition due to privacy issues. In China, there was a system of providing ID cards, containing very basic information, since 1985. In 2003, the card was legally updated for law and order purposes and comprised of a chip storing additional information. By 2004, the government introduced the “second generation” mandatory ID cards, which had a small storage capacity, therefore restricting information to name, gender, ethnicity, residence and date of birth - but decided against it as this huge system was found to be very challenging to handle and of doubtful reliability.

Given this context, it becomes glaringly obvious just how pervasive and intrusive the UID system is set to be, far more than any of the systems that have been rejected elsewhere. Some people argue that just because countries like the US, UK and Australia were not able to implement or simply scrapped similar programmes, doesn't mean India cannot do it - India can be a leader in implementing such an ambitious programme. But then again, isn't it sensible for a "global" nation like India to learn from the experiences of other countries - the very same ones a section of the population believes India aspires to be like?

## **END NOTE**

It is important to understand that implementing a national ID system of this magnitude is poised to alter the way we live as well as the relationship between the citizen and the state. As Graham Greenleaf, an Australian data protection expert and one of the pioneers of the anti-ID card movement, puts it: “Is it realistic to believe that the production of identity cards

by children to adults in authority to prove their age will be ‘purely voluntary’? The next generation of children may be accustomed to always carrying their Cards, to get a bus or movie concession, or to prove they are old enough to drink, so that in adult life they will regard production of an ID card as a routine aspect of most transactions.”

The UID project has the potential of being a financially exorbitant and socially invasive debacle, given that it is the largest national ID card project in the world, in scale and scope. Instead of the government becoming more accountable to its citizens, this system lays the burden on the governed. Of course, if the project succeeds, it may have useful applications too. But does this justify the kind of intrusion that UID is set to create into people’s lives? Perhaps what would help is a meaningful dialogue with various sections of society, with ample space to debate the implications of such a project and even reconsider it.

## References

- Bidwai, Praful (2010), "Why Indians Should Fear the UID", *Rediff News*, 12<sup>th</sup> October 2010 ([www.rediff.com/news/column/column-why-indians-should-fear-the-uid/20101012.htm](http://www.rediff.com/news/column/column-why-indians-should-fear-the-uid/20101012.htm)).
- Drèze, Jean (2010), "UID: Unique Facility or Recipe for Trouble?", *The Hindu*, 25<sup>th</sup> November 2010.
- Harlarnkar, Samar (2010), "Play it again, Sam", *Hindustan Times*, 11 October (<http://epaper.hindustantimes.com/PUBLICATIONS/HT/HD/2010/10/11/ArticleHtmls/Play-it-again-Sam-inclusivepolitics-11102010013002.shtml?Mode=1>).
- Himanshu (2010), "The Foundations of Aadhaar", *Livemint*, 5<sup>th</sup> September 2010. ([www.livemint.com/2010/09/15004015/The-foundations-of-Aadhaar.html](http://www.livemint.com/2010/09/15004015/The-foundations-of-Aadhaar.html)).
- Khera, Reetika (2010), "Not all that unique", *Hindustan Times*, 30<sup>th</sup> August 2010.
- Khera, Reetika (2011), "The UID Project and Welfare Schemes", *Economic and Political Weekly*, 4<sup>th</sup> March 2010.
- Lerner, Mark (2010), "The Revolving Door that Never Stops Turning", November 2010 (<http://americanpolicy.org/more-issues/the-revolving-door-that-never-stops-turning.html>).
- London School of Economics and Political Science (2005), *The Identity Project: An assessment of the UK Identity Cards Bill and its Implications* (London: London School of Economics and Political Science).
- Mittal, Tusha (2009), "Falling Between the Bar Codes", *Tehelka*, 22<sup>nd</sup> August.
- Planning Commission (2004), "A Study of the Effectiveness of Public Distribution System in Rural Tamil Nadu" ([http://planningcommission.nic.in/reports/sereport/ser/std\\_pdstn.pdf](http://planningcommission.nic.in/reports/sereport/ser/std_pdstn.pdf)).
- Ramanathan, Usha (2010a), "Implication of Registering, Tracking, Profiling", *The Hindu*, 5<sup>th</sup> April.
- Ramanathan, Usha (2010b), "A Unique Identity Bill", *Economic and Political Weekly*, 24<sup>th</sup> July.
- Ramanathan, Usha (2011), "The Personal is the Personal," *Indian Express*, 6 January ([www.indianexpress.com/news/the-personal-is-the-personal/563920/0](http://www.indianexpress.com/news/the-personal-is-the-personal/563920/0)).
- Rao, Mohan (2010), "UID and Public Health: Magic Bullet or Poison Pill?", *The Asian Age*, 24<sup>th</sup> December ([www.asianage.com/ideas/uid-public-health-magic-bullet-or-poison-pill-977](http://www.asianage.com/ideas/uid-public-health-magic-bullet-or-poison-pill-977)).
- Shorrock, Tim (2007), "George Tenet cashes in on Iraq", 7<sup>th</sup> May 2007 ([http://www.salon.com/news/feature/2007/05/07/tenet\\_money](http://www.salon.com/news/feature/2007/05/07/tenet_money)).
- Shukla, Ravi (2010), "Reimagining Citizenship: Debating India's Unique Identification Scheme", *Economic and Political Weekly*, 9<sup>th</sup> January.
- UIDAI, "UIDAI Strategy Overview: Creating a unique identity number for every resident in India", available at <http://uidai.gov.in>
- UIDAI, "Registrar FAQ's: Summary of responses to Questions Frequently Asked by Registrars", available at <http://uidai.gov.in>
- UID Project (Aadhar) Issue Overview

“Lockheed Martin ends association with Wipro in network centric warfare project”,  
Defenseworld.net, February 11<sup>th</sup>, 2009  
(<http://www.defenseworld.net/go/defensenews.jsp?n=Lockheed%20Martin%20ends%20association%20with%20Wipro%20in%20network%20centric%20warfare%20project&id=2756>)

“Lockheed Martin, Wipro To Light Ambar Jyoti In India”, EFYTimes.com, August 13<sup>th</sup>,  
2007 (<http://www.efytimes.com/e1/fullnews.asp?edid=20995>)

“UIDAI rolls out 10 Lakh ‘Aadhaar’ Numbers”, Times of India, January 13<sup>th</sup>, 2011  
([http://articles.timesofindia.indiatimes.com/2011-01-13/india/28370904\\_1\\_aadhaar-enrolments-unique-identification-number](http://articles.timesofindia.indiatimes.com/2011-01-13/india/28370904_1_aadhaar-enrolments-unique-identification-number))

Additional Links:

<http://frontierindia.net/lockheed-martin-team-wins-role-on-key-department-of-defense-biometrics-contract-vehicl>

<http://frontierindia.net/mahindra-satyam-and-morpho-selected-to-develop-and-maintain-systems-for-unique-identification-authority-of-india>

<http://timesofindia.indiatimes.com/tech/enterprise-it/infrastructure/Intel-forms-open-data-centre-alliance/articleshow/6829123.cms>

## **Appendix 1**

### **Valid Identification Documents**

A range of identification cards/documents were in use before the UID came into the scene. They are listed below, along with the information they contain:

#### **Documents Containing Name and Photo**

1. Passport
2. PAN Card
3. Ration/ PDS Photo Card
4. Voter ID
5. Driving License
6. Government Photo ID Cards
7. NREGS Job Card
8. Photo ID issued by Recognized Educational Institution
9. Arms License
10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kissan Photo Passbook
15. CGHS / ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identify having photo issued by Group A Gazetted Officer on Letterhead

#### **Documents Containing Name and Address**

1. Passport
2. Bank Statement/ Passbook
3. Post Office Account Statement/Passbook
4. Ration Card
5. Voter ID
6. Driving License
7. Government Photo ID cards
8. Electricity Bill (not older than 3 months)
9. Water bill (not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property Tax Receipt (not older than 3 months)
12. Credit Card Statement (not older than 3 months)
13. Insurance Policy
14. Signed Letter having Photo from Bank on letterhead
15. Signed Letter having Photo issued by registered Company on letterhead
16. Signed Letter having Photo issued by Recognized Educational Institution on letterhead
17. NREGS Job Card
18. Arms License
19. Pensioner Card
20. Freedom Fighter Card
21. Kissan Passbook
22. CGHS / ECHS Card

23. Certificate of Address having photo issued by MP or MLA or Group a Gazetted Officer on letterhead
24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
25. Income Tax Assessment Order
26. Vehicle Registration Certificate
27. Registered Sale / Lease / Rent Agreement
28. Address Card having Photo issued by Department of Posts
29. Caste and Domicile Certificate having Photo issued by State Govt.

**Proof of Date of Birth Documents**

1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on letterhead



## **Appendix 2**

### **ID Systems and Debates across the World**

Improvements in technology have radically altered the pace at which systems of identification have developed all over the world. Taking lessons from the experiences of other nations who've taken similar paths, or not, would serve well before the mammoth task of implementing UID amongst a population of over a billion, is undertaken.

#### **European Countries**

Most European Union members have voluntary and compulsory ID cards except Denmark, Latvia and Lithuania. In Sweden, information is stored on a chip in the card and not in any central database.

#### **France**

The national identity card (Carte Nationale D'identité Sécurisée or CNIS) of France is an official non-compulsory identity document consisting of a plastic card bearing a photograph, name and address.

The fingerprints of the card holder are stored in paper file and are only accessible to judges in extreme circumstances. The information on the card is duplicated in a central database but access is limited by strict laws and is not linked to any other records. The card is often used to verify nationality and for travelling within the EU. Following a study launched in 2001, the government planned to introduce a new card the INES (carte d'identité nationale électronique sécurisée) also known as "secure electronic national identity card", that would contain biometric fingerprints and photograph data on a chip which would be recorded on a central database. A group of French bodies initiated a report and petition against the plans. Although draft legislation was published in 2005, the government has yet to set a date for a discussion of the proposals in the Parliament.<sup>55</sup>

#### **Germany**

In Germany, it is compulsory for all citizens, 16 years or above, to possess either a Personalausweis (identity card) or a passport, but it's not necessary to carry one. While authorities have a right to demand to see one of those documents, the law does not state that it is necessary for one to submit the document at that very moment. But most Germans carry their Personalausweis with them as driver's licences are not legally accepted forms of identification in Germany.<sup>56</sup>

Beginning in November 2010, German ID cards contain RFID chips with personally identifiable information including a biometric Photo and, if desired, two fingerprints. The German government's new national ID card was publicly hacked on TV by members of the infamous Chaos Computer Club. Members of the Chaos Computer Club demonstrated how easy the cards were to crack live on the WDR TV channel. The hackers cracked the PIN system on the cards, which then allowed them to impersonate the cardholder online. Germany's Federal Office for Information Security acknowledged that the card's PIN can be cracked using trojan malware, similar to keylogging software.<sup>57</sup>

## **United Kingdom**

The government's attempts to impose compulsory ID cards sparked off fury early this year. The Home Affairs committee shot down the idea as its benefits outweighed the increased data protection risks. In July 2002, David Blunkett, Former Labour Home Secretary had initiated plans for an identity card scheme. By February 2010, the government scrapped the plan as the scheme's overall cost massively inflated to an estimated £4.5bn. These cards were intended to hold biometric data such as name, fingerprints and a photograph on an encrypted chip. Apart from this, the National Identity Register was designed to hold up to 50 different types of personal information. These identity cards were aimed at tackling illegal immigration, fraud and identity theft - but eventually were abandoned after they were criticised for infringing civil liberties and being too expensive. After the plans were abandoned, personal information of 15,000 people who applied for an ID card before the scheme was cancelled, were systematically **destroyed** (not disabled) by the British government.<sup>58</sup>

## **Bosnia**

The Bosnian government pushed for a national ID in 2002, with the stated intention of promoting unity. The technology under usage includes a bar code instead of a chip on the card along with a photograph, signature and a single fingerprint. It decided against using a smart card chip.

## **United States of America**

The Social Security programme number is also used as the national identification number. But attempts at introducing biometric national cards have come under fire from rights groups.

45 organizations representing privacy, consumer, civil liberty and civil rights organizations joined together and launched a nation wide campaign to garner public support to stop America's first national ID system: REAL ID. The Real ID Act of 2005 was the result of recommendations of the 9/11 Commission and was passed as part of anti-terrorism effort. This act would've allowed all driver's licenses to be linked, leading to a person's records to be accessible by officials in other states and federal agencies. Although initially it wasn't mandatory for states to issue Real ID Cards, the Department of Homeland Security eventually wanted Real ID cards to be required for air travel and for receiving benefits such as Social Security.<sup>59</sup>

This card would've included identity documents such as a photo ID, documentation of birth date and address, proof of citizenship or immigration status and verification of Social Security numbers. The states were required to hold digital images of each identity document for periods ranging from seven to 10 years. The groups opposing this measure were concerned about the increased threat of counterfeiting and identity theft, lack of security to protect against unauthorized access to the content, cost burden on the taxpayers, diversion of funds meant for homeland security, increased costs for obtaining a license or state issued ID card, and because Real ID would create a false image that it is secure and impenetrable.

Even a couple of the most vocal senators on implementing national ID, Sen. Charles Schumer (D-New York) and Sen. Lindsay Graham (R-South Carolina) said that, "We would require all U.S. citizens and legal immigrants who want jobs to obtain a high-tech, fraud-proof Social

Security card. Each card's unique biometric identifier would be stored only on the card; no government database would house everyone's information,"<sup>60</sup>

Despite this, many civil society activists and citizens voiced their intense disapproval for such a measure. Jim Harper, Director of Information Policy Studies at the Cato Institute, believed that the plan would undoubtedly lead to a national database. He added that "there is no practical way of making a national identity document fraud-proof."

By October 2009, 25 states approved resolutions not to participate in the programme. The resolution passed in Utah stated that Real ID is "in opposition to the Jeffersonian principles of individual liberty, free markets, and limited government." It further states that "the use of identification-based security cannot be justified as part of a 'layered' security system if the costs of the identification 'layer'--in dollars, lost privacy, and lost liberty--are greater than the security identification provides".

As a compromise, the Obama administration introduced Pass ID in the Congress. The Pass ID Act sets strong security standards for the issuance of identification cards and driver's licenses. On the other hand, it does not collect personal information of individuals and store it in a centralized database, accessible by any state authority.<sup>61</sup>

## **Canada**

It had a short-lived deliberation over adopting national ID cards. But after an interim report the Canadian Government is moving to implement biometric passports. Although the national ID card plan was dumped officially in March 2004, in April 2004 the Government announced its plans for biometric passports.

## **Pakistan**

Since the 1960s, Pakistan has been issuing National Identity Card (NIC) numbers to its citizens. Established in the year 2000, the National Database and Registration Authority (NADRA) is Pakistan's state-owned IT services company that specializes in implementing multi-biometric national identity cards and e-passports, as well as secure access verification and control systems in both public and private sectors. In fact, what is not widely some reports originating from the Planning Commission raised questions about UIDAI ignoring not just privacy concerns, but also the sample test results. So far, data results from just 20,000 people has been the basis for over 1.2 billion UID numbers known is that Pakistan is amongst the first few countries in the world to attempt to issue national ID biometric cards and e-passports to its citizens (Pakistan has also issued over 7 million e-passports to its citizens since October, 2004)<sup>62</sup>. In February 2006, the Authority had issued its 50 millionth Computerized National Identity Card. However, the picture ain't as rosy as it seems. The NADRA is dogged with allegations about tricksters having a ball with this programme and getting away with creating fake ID cards in huge numbers. Another sticky issue is that of Afghan refugees living in Pakistan and what consequence giving them Pakistani nationality would lead to.<sup>63</sup>

## **Malaysia**

The country has always had a national ID card, but in 2001, moved to replace the existing card and driving licenses with a smart card containing a 64k chip called the MyKad or the

Malaysian Card. This chip contains a thumbprint and other personal information, including basic health details. It is presently a world leader on identity systems.

## **Japan**

The government's national ID plans took the form of Juki Net, a Basic Resident Registration Network in 1999(it was a voluntary card with a unique 11 digit number) that had a tumultuous start, and was faced with a lot of protests over security issues and had to deal with quite a few court cases filed on the basis of unconstitutionality. However in 2008, the ID system got the go ahead after its constitutionality was established by the Supreme Court

## **Taiwan**

Taiwan had been trying to implement biometric identification system for quite some time. But a move to incorporate fingerprints in the card was met with fierce opposition. Aside from privacy implications, fingerprinting was deemed indecisive in solving criminal cases. The Vice President of the time, Annette Lu, felt that the fingerprint condition in the ID was unconstitutional and would undermine the nation's democratic credentials by stating that, "The government's collection and storage of fingerprint records constitutes a collection of individual data and involves the questions of guarantees of the individual right of privacy and information autonomy."

## **People's Republic of China**

The Chinese government had implemented a system of providing ID cards, containing very basic information to every citizen since 1985. In 2003, the card was legally updated to verify citizens' identity and law and order purposes and comprised of a chip that stores additional information. By 2004, the government introduced the "second generation" mandatory ID cards, involving contact less chips containing a small storage capacity (4k- therefore, restricting information to name, gender, ethnicity, residence and date of birth).

They deliberated on incorporating fingerprints but decided against it as they found the system to be very challenging to handle and had reservations about its reliability. Seemingly, biometrics overwhelm a system of this nature. "Such an effort to introduce biometrics, the huge quantity (of cardholders), is not feasible," said an official from the Chinese National Registration Centre.

Early this year, China began issuing smart cards to its citizens. The cards can also help identify those who use ATMs, enter a building with an electronic guard system or even pick up their children from kindergarten.

## **Australia**

After the Second World war ended, the national cards were withdrawn. The issue of national ID cards was raised 30 years later and after a few government inquiry reports, dropped the idea. It resurfaced in 1985, when the government proposed Australian cards, mostly to curb tax evasion. Australia probably witnessed the most forceful protests and campaigns against a national ID proposal. Following a vigorous opposition campaign, the proposal was withdrawn in 1987. Though Australia is including biometrics in passports, it is limited to a digital photograph.

## **West Asia**

According to reports, Oman, UAE, Saudi Arabia and Israel are drawing up plans of issuing “smart” ID cards, with Oman taking the lead and the card it issues will store fingerprints. The purpose behind issuing these cards in the country is primarily immigration management. Even though the Oman government is planning multiple applications on the card, however, information on the card cannot be disseminated to all government agencies nor to the private sector.

## Notes

- <sup>1</sup> Srinivasaraju, Sugata, “Biometry Is Watching”, Outlook, 17<sup>th</sup> May, 2010 (<http://www.outlookindia.com/article.aspx?265326>)
- <sup>2</sup> Narendra Kaushik (2011), "Cards to Nowhere", *Inclusion*, April-June 2011.
- <sup>3</sup> Gupta, Vishv, “What the UID project will not do”, Tehelka, 2<sup>nd</sup> June, 2011 ([http://www.tehelka.com/story\\_main49.asp?filename=Ws020611UIDproject.asp](http://www.tehelka.com/story_main49.asp?filename=Ws020611UIDproject.asp))
- <sup>4</sup> UIDAI, “UIDAI Strategy Overview: Creating a unique identity number for every resident in India”, available at [http://uidai.gov.in/UID\\_PDF/Front\\_Page\\_Articles/Documents/Strategy\\_Overveiw-001.pdf](http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf)
- <sup>5</sup> PRS India, “The National Identification Authority of India Bill, 2010”, available at <http://prsindia.org/uploads/media/UID/The%20National%20Identification%20Authority%20of%20India%20Bill,%202010.pdf>
- <sup>6</sup> UIDAI, “UIDAI Strategy Overview: Creating a unique identity number for every resident in India”, available at [http://uidai.gov.in/UID\\_PDF/Front\\_Page\\_Articles/Documents/Strategy\\_Overveiw-001.pdf](http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf)
- <sup>7</sup> Mittal, Tusha, “Falling Between the Bar Codes”, Tehelka, August 22<sup>nd</sup>, 2009. ([http://www.tehelka.com/story\\_main42.asp?filename=Ne220809falling\\_between.asp](http://www.tehelka.com/story_main42.asp?filename=Ne220809falling_between.asp))
- <sup>8</sup> Moneylife.in, “No card, only a number despite Rs. 45,000 crore being spent on the UID project”, available at <http://www.moneylife.in/article/8/6920.html>
- <sup>9</sup> See <https://portal.uidai.gov.in/uidwebportal/dashboard.do>
- <sup>10</sup> Bidwai, Praful, “Why Indians Should Fear the UID”, Rediff News, October 12<sup>th</sup>, 2010 <http://www.rediff.com/news/column/column-why-indians-should-fear-the-uid/20101012.htm>
- <sup>11</sup> Editor’s Guild of India’s Annual Rajinder Mathur Memorial Lecture attended by writers of this primer (<http://expressbuzz.com/nation/each-unique-id-number-costs-rs100-nilekani/227888.html>)
- <sup>12</sup> Dreze, Jean, Unique Facility or Recipe for Trouble, The Hindu, November 25th, 2010
- <sup>13</sup> Sanyal, Kaushiki and Kumar, Rohit (2011), “The National Identification Authority of India Bill (2010)”, PRS Legislative Research, June 2nd, 2011 (<http://indialawyers.wordpress.com/2011/06/19/the-national-identification-authority-of-india-bill-2010/>)
- <sup>14</sup> Justice.gov, Overview of the Privacy Act of 1974, 2010 Edition, (<http://www.justice.gov/opcl/1974ssnu.htm>)
- <sup>15</sup> UIDAI, “Registrar FAQ’s: Summary of responses to Questions Frequently Asked by Registrars”, available at <http://uidai.gov.in/images/FrontPageUpdates/ROB/A2%20Registrar%20FAQs.pdf>
- <sup>16</sup> Sethi, Nitin, “NGO’s shelter shut after it pointed out UID flaws”, Times of India, 4th July 2011, [http://articles.timesofindia.indiatimes.com/2011-07-04/india/29735661\\_1\\_uid-enrolment-ngo-igsss](http://articles.timesofindia.indiatimes.com/2011-07-04/india/29735661_1_uid-enrolment-ngo-igsss)
- <sup>17</sup> UIDAI, “UIDAI Strategy Overview: Creating a unique identity number for every resident in India” available at [http://uidai.gov.in/UID\\_PDF/Front\\_Page\\_Articles/Documents/Strategy\\_Overveiw-001.pdf](http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf)
- <sup>18</sup> UIDAI, “UID and NREGA” ([http://uidai.gov.in/UID\\_PDF/Working\\_Papers/UIDandNREGA.pdf](http://uidai.gov.in/UID_PDF/Working_Papers/UIDandNREGA.pdf)).
- <sup>19</sup> Agarwal, Surabhi, “UID Puts Revenue Stream on Hold”, Livemint, 16th February, 2011 (<http://www.livemint.com/2011/02/16010317/UID-puts-revenue-stream-on-hol.html?atype=tp>)
- <sup>20</sup> UIDAI, “UID and NREGA” ([http://uidai.gov.in/images/FrontPageUpdates/uid\\_and\\_mgnrega.pdf](http://uidai.gov.in/images/FrontPageUpdates/uid_and_mgnrega.pdf)).
- <sup>21</sup> On the issue of corruption and the transition to bank and post office payment of NREGA wages, see Siddharth and Vanaik (2008), Dreze and Khera (2008), and Adhikari and Bhatia (2010).
- <sup>22</sup> “UID Project (Aadhar) Issue Overview”,
- <sup>23</sup> See <http://www.sacw.net/article1722.html>.
- <sup>24</sup> UIDAI, “UID and PDS System”, available at [http://uidai.gov.in/images/FrontPageUpdates/uid\\_and\\_pds.pdf](http://uidai.gov.in/images/FrontPageUpdates/uid_and_pds.pdf)

---

25 See various documents posted on the website of the right to food campaign ([www.righttofoodindia.org](http://www.righttofoodindia.org)); also the recent “open letter” to the Prime Minister on this subject, based on a survey of the PDS in nine states (<http://www.sacw.net/article2207.html>).

26 Thaindian News, “Lacking Healthcare, A Million Indians Die Every Year”, 2nd February, 2009 ([http://www.thaindian.com/newsportal/world-news/lacking-healthcare-a-million-indians-die-every-year-oxford-university\\_100150164.html](http://www.thaindian.com/newsportal/world-news/lacking-healthcare-a-million-indians-die-every-year-oxford-university_100150164.html))

27 UIDAI, “UID and Public Health”, ([http://uidai.gov.in/UID\\_PDF/Working\\_Papers/UIDandPublicHealth.pdf](http://uidai.gov.in/UID_PDF/Working_Papers/UIDandPublicHealth.pdf))

28 Rao, Mohan, “UID and Public Health: Magic Bullet or Poison Pill”, The Asian Age, 24th December, 2010 (<http://www.asianage.com/ideas/uid-public-health-magic-bullet-or-poison-pill-977>)

29 Pato and Millette (2010), “Biometric Recognition: Challenges and Opportunities”

30 Dr. Kamlesh Bajaj, “Security and Privacy Challenges in the Unique Identification Project,” Project RISE (A NASSCOM initiative) 25th March, 2010

31 Ton van der Puetter and Jeroen Keuning “Biometrics and Fingerprints”, (<http://keuning.com/biometry/>)

32 London School of Economics and Political Science (2005), The Identity Project: An assessment of the UK Identity Cards Bill and its Implications (London: London School of Economics and Political Science).

33 Also refer to Drèze, Jean (2010), "UID: Unique Facility or Recipe for Trouble?", The Hindu, 25 November (<http://www.hindu.com/2010/11/25/stories/2010112563151300.htm>)

34 Kakatkar-Kulkarni, Manasi, “Chidambaram proposes radical restructuring of India's security structure”, Foreign Policy Association, December 23<sup>rd</sup>, 2009 (<http://india.foreignpolicyblogs.com/2009/12/23/chidambaram-proposes-radical-restructuring-of-indias-security-structure/>)

35 Pandey, Brijesh, “Natgrid will kick in from May 2011. Is the big brother threat for real?”, November 13th, 2010 ([http://www.tehelka.com/story\\_main47.asp?filename=Ne131110Natgrid\\_will.asp](http://www.tehelka.com/story_main47.asp?filename=Ne131110Natgrid_will.asp)). Also refer to (<http://news.rediff.com/report/2010/feb/06/natgrid-will-track-all-your-spending.htm>)

36 Times News Network, “CCS seeks tighter privacy safeguards in NATGRID proposal,” Times of India, February 11th, 2010 (<http://timesofindia.indiatimes.com/india/CCS-seeks-tighter-privacy-safeguards-in-NATGRID-proposal/articleshow/5557716.cms#ixzz1B8WSNJ9e>)

37 Governance Now, “Fin min says no to Natgrid spying on bank account-holders”, 27th September 2010, (<http://www.governancenow.com/news/regular-story/fin-min-says-no-natgrid-spying-bank-account-holders>)

38 Hindustan Times, “Cabinet clears creation of National Population Register”, 19th March 2010, (<http://www.hindustantimes.com/Cabinet-clears-creation-of-National-Population-Register/Article1-521016.aspx>)

39 “Aadhar: Pied Piper of Technology”, Inclusion, April- June 2011 ([http://www.inclusion.in/index.php?option=com\\_content&view=article&id=669:cover-story&catid=234:editor](http://www.inclusion.in/index.php?option=com_content&view=article&id=669:cover-story&catid=234:editor))

40 Dhoot, Vikas, “Nandan Nilekani's UIDAI and Census' NPR in role overlap for fingerprinting and other biometric data”, Economic Times, 11<sup>th</sup> August 2011 (<http://m.economictimes.com/PDAET/articleshow/9560067.cms>)

41 Rahman, Shafi, “Unique ID project hits legal hurdle”, India Today, 25th July 2010, (<http://indiatoday.intoday.in/site/story/unique-id-project-hits-legal-hurdle/1/144988.html>)

42 Ramanathan, Usha, “Implications of registering, tracking and profiling”, The Hindu, 4th April, 2010 (<http://www.thehindu.com/opinion/lead/article388037.ece>)

43 Zaba, Christina, “When the eyes don't have it,” New Statesman, 30th May, 2010 (<http://www.newstatesman.com/200505300020>). Also refer to <http://nprindia.blogspot.com/search?updated-min=2008-01-01T00:00:00-08:00&updated-max=2009-01-01T00:00:00-08:00&max-results=9>

- 
- 44 Ramanathan, Usha, "A Unique Identity Bill", Economic and Political Weekly, VOL XLV NO 30, July 24, 2010
- 45 Ramanathan, Usha, "The Personal is the personal", Indian Express, 6th January, 2011 (<http://www.indianexpress.com/news/the-personal-is-the-personal/563920/0>)
- 46 Soni, Raghav, "Govt Set To Create Massive Domestic IT Opportunities Through UID", Watblog.com, 29th June, 2009, (<http://www.watblog.com/2009/06/29/govt-set-to-create-massive-domestic-it-opportunities-through-uid/>)
- 47 Govindasswamy, Majoj, "Infosys, TCS, IBM, HCL ... ? Who's gonna build World's largest biometric database? UID Software Tender!" Moneymint.in, 29th March, 2010 (<http://www.moneymint.in/corporates/infosys-tcs-ibm-hcl-whos-gonna-build-worlds-largest-biometric-database-uid-software-tender>)
- 48 Shorrock, Tim, "George Tenet cashes in on Iraq", Salon.com, 7th May, 2007 ([http://www.salon.com/news/feature/2007/05/07/tenet\\_money](http://www.salon.com/news/feature/2007/05/07/tenet_money))
- 49 Abraham, Jacob, "The Strange Case of Identity Outsourcing", Zeebiz.com, 2nd February, 2011 (<http://biz.zeenews.com/interviews/story.aspx?newsid=258>)
- 50 , Mark, "The Revolving Door that Never Stops Turning", American Policy Center, November, 2010 (<http://americanpolicy.org/more-issues/the-revolving-door-that-never-stops-turning.html>)
- 51 Shukla, Ravi, "Reimagining Citizenship: Debating India's Unique Identification Scheme", Economic and Political Weekly, VOL XLV NO 2, January 9th, 2010
- 52 Moneylife.in, "UID = more 'consumers', admits Nilekani", 25th November 2010 (<http://www.moneylife.in/article/78/11574.html>)
- 53 Chari, Sridhar, "Sensor technologies to be the new growth driver for Infosys", Mint, 30th November 2010 (<http://www.livemint.com/2010/11/30221149/Sensor-technologies-to-be-the.html>)
- 54 RNCOS, "Consumer ID to Drive Global Biometric Market", prlog.org, March 2011 (<http://www.prlog.org/10658907-consumer-id-to-drive-global-biometric-market.html>). Also see <http://www.uidaicards.com/?p=1624>
- 55 Marzouki, Meryam, "French NGOs: no consensus possible on biometric ID-card", INES, 29th June, 2005 (<http://www.ines.sgdg.org/spip.php?article17>). Also refer to - [http://www.servinghistory.com/topics/National\\_identity\\_card\\_\(France\)](http://www.servinghistory.com/topics/National_identity_card_(France)) ; and [http://news.bbc.co.uk/2/hi/uk\\_news/politics/2078604.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/2078604.stm))
- 56 Wessel, Rhea, "Germany Gets Set to Issue RFID ID Cards and Readers to Its Citizens", RFID Journal, 6th October 2010, (<http://www.rfidjournal.com/article/view/7927>)
- 57 Infosecurity.com, "New German national ID card hacked by Chaos Computer Club", 30th September 2010 (<http://www.infosecurity-magazine.com/view/12859/new-german-national-id-card-hacked-by-chaos-computer-club/>). Also see - <http://boingboing.net/2010/09/02/german-secure-id-car.html>
- 58 Casciani, Dominic, "Q&A: Identity Cards", BBC News, 27th May 2010 ([http://news.bbc.co.uk/2/hi/uk\\_news/politics/8708054.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/8708054.stm)). Also refer to -<http://www.bbc.co.uk/news/uk-politics-11719764>
- 59 The Privacy Coalition, "Over Forty Groups Announce National REAL ID Public Campaign", (<http://privacycoalition.org/stopenrealid/pressrelease.php>)
- 60 Kravets, David, "Lawmakers Eyeing National ID Card", Wired.com, 23rd March, 2010 (<http://www.wired.com/threatlevel/2010/03/two-id-cards/>). Also refer to - ([http://www.wired.com/threatlevel/2009/12/real\\_id/](http://www.wired.com/threatlevel/2009/12/real_id/))
- 61 Jaikumar, Vijayan, "Privacy Groups Renew Push Against Real ID Bill", PC World, 4<sup>th</sup> May 2010, ([http://www.pcworld.com/article/131560/privacy\\_groups\\_renew\\_push\\_against\\_real\\_id\\_bill.html](http://www.pcworld.com/article/131560/privacy_groups_renew_push_against_real_id_bill.html)). Also refer to



---

- ([http://www.computerworld.com/s/article/print/9204858/Real\\_ID\\_alive\\_and\\_kicking\\_report\\_says](http://www.computerworld.com/s/article/print/9204858/Real_ID_alive_and_kicking_report_says)); and (<http://www.govtech.com/security/99354049.html> )

62 The Dawn, “Pakistan Has World’s Largest Biometric Citizen Database”, 1<sup>st</sup> November, 2009 ([http://www.nadra.gov.pk/index.php?option=com\\_content&view=article&id=142:pakistan-has-worlds-largest-biometric-citizen-database&catid=10:news-a-updates&Itemid=20](http://www.nadra.gov.pk/index.php?option=com_content&view=article&id=142:pakistan-has-worlds-largest-biometric-citizen-database&catid=10:news-a-updates&Itemid=20)). Also see: <http://www.riazhaq.com/2011/05/pakistan-leads-asia-in-biometric-it.html>

63 Ghumman, Khawar, “PAC to take up issue of fictitious ID cards today”, The Dawn, 19<sup>th</sup> March, 2011 (<http://www.dawn.com/2011/03/19/pac-to-take-up-issue-of-fictitious-id-cards-today.html>).

Also check:

<http://www.dawn.com/2011/03/20/afghan-refugees-a-problem-for-nadra.html>