The Unique ID Project in India: A Skeptical Note

R. Ramakumar

School of Social Sciences,
Tata Institute of Social Sciences, Mumbai – 400 088
rr@tiss.edu

Abstract. In this note, I discuss certain social and ethical aspects of a new national project to supply unique ID (UID) numbers to Indian residents. The UID project is presented as a "technology-based solution" that would change the face of governance in India. I argue in this note that the UID project would actually lead to the violation of a large number of freedoms of Indian people. No amount of assertion vis-à-vis improved service delivery can justify the violation of citizen's freedoms and liberties. Next, I argue that there is a misplaced emphasis on the benefits of technology in this project, when the robustness of that technology to handle large populations remains largely unproven. Further, I argue that no detailed cost-benefit analysis of the project has been carried out yet. Finally, I try to show, with an illustration, that the roots of inefficiency in public welfare schemes in India are policy-induced and do not lie in the absence of identity proofs.

Keywords: Identity Cards, Unique Identification Numbers, Technology and Governance, ICT, India.

1 Introduction

The intensified use of science and technology in matters of public administration and governance is a phenomenon of the 1980s and after. While many basic facets of technology, such as photography, have been used in governance earlier as well, the use of high-end forms of information and communication technology (ICT) like centralized national databases, biometrics and satellite imageries are more recent. Concurrently, there has been much euphoria in the mainstream literature on governance regarding the impacts of ICT on the evolution of societies and their socio-economic development (see Friedman, 2005) [1].

On the other hand, a parallel stream of literature has argued that it may be erroneous to assume a simple linear relationship between the development of technology and the development of society. This literature, while looking at the growth in productive forces as integral to the evolution of humanity itself, underlines the complex and intimate intertwining of society and technology. These studies call for a detailed understanding of how technology and social relations interact and caution against viewing it as a simple cause-and-effect sequence. Thus, in the study of e-governance initiatives as well as projects that involve intensive utilization of ICT, social scientists try to emphasise the study of society itself as a starting point. Yet, notwithstanding

A. Kumar and D. Zhang (Eds.): ICEB 2010, LNCS 6005, pp. 153–167, 2010.

this literature, governments across the world have tended to see hastened adoption of ICT in governance as a panacea to the problems of inefficiencies in administration and service delivery.

2 The Unique ID (UID) Project in India

In this note, I discuss certain social and ethical aspects of a new national project to supply unique ID numbers to Indian residents. In 2009, soon after assuming power, the new Indian government announced the formation of the Unique Identification Authority of India (UIDAI) and appointed Nandan Nilekani (formerly the Chairman of INFOSYS, a private corporate information technology and consulting firm), as its Chairperson. As per a working paper of the UIDAI, the Authority proposes 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" (UIDAI, 2009a, pp. 4-5). The UIDAI is envisaged to enroll all Indian residents into a centralized database, along with their demographic and biometric (fingerprint and IRIS scans) information. It is argued by the UIDAI that there are

> …immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies… This will result in significant savings to the state exchequer (UIDAI, 2009a, p. 1).

In other words, the UID project appears to have been envisaged as from a clear developmental angle rather than a security angle, as was the case in earlier attempts to issue citizen identity cards. In fact, the original project to issue unique ID cards to Indian citizens was initiated by the right-wing National Democratic Alliance (NDA) government that was in power between 1999 and 2004. The first steps to issue unique ID cards began with the controversial report of the *Kargil Review Committee* in 1999, appointed in the wake of the Kargil War between India and Pakistan [2]. In its report submitted in January 2000, this Committee had noted that immediate steps were needed to issue ID Cards to villagers in border districts, pending its extension to other parts of the country.

In 2001, a Group of Ministers (GoM) submitted a report to the government titled *Reforming the National Security System*. This report was based largely on the findings of the Kargil Review Committee. The report noted that:

> Illegal migration has assumed serious proportions. There should be compulsory registration of citizens and non-citizens living in India. This will facilitate preparation of a national register of citizens. All citizens should be

> given a Multi-purpose National Identity Card (MNIC) and non-citizens should be issued identity cards of a different colour and design.

In 2003, the NDA government initiated a series of steps to ensure the smooth preparation of the national register of citizens, which was to form the basis for the preparation of ID cards. It was decided to link the preparation of this register with the decennial census surveys of India. However, the Census of India has always had very strong clauses related to the privacy of its respondents. Thus, the Citizenship Act of 1955 was amended in 2003, soon after the MNIC was instituted. This amendment allowed for the creation of a post of Director of Citizen Registration, who was also to function as the Director of Census in each State. According to the citizenship rules notified on 10 December 2003, the onus for registration was placed on the citizen himself: "it shall be compulsory for every Citizen of India to…get himself registered in the Local Register of Indian Citizens [3]." The rules also specified punishments for citizens who fail to do so; any violation was to be "punishable with fine, which may extend to one thousand rupees." Thus, the privacy clauses in Census surveys were diluted significantly in 2003 itself.

The first UPA government that came to power in 2004 carried forward the plans of the NDA government under a new name. The MNIC project was replaced by the UID project in January 2009. Indicating a shift from a security angle to a developmental angle, a press release of the government dated 10 November 2008 noted that UID project would serve a variety of purposes: "better targeting of government's development schemes, regulatory purposes (including taxation and licensing), security purposes, banking and financial sector activities, etc [4]." According to the government, the UID will be "progressively extended to various government programmes and regulatory agencies, as well as private sector agencies in the banking, financial services, mobile telephony and other such areas."

A number of similar claims have been made by Nandan Nilekani after taking charge as the Chairman of the UIDAI; according to news reports, he has argued that the UID would make it possible to open a bank account in India with no supporting documents, thus expanding "financial inclusion [5]"; the UID would make it easier to obtain a mobile telephone connection than at present [5]; the UID would ensure that the public food distribution system (PDS) in India would cease to be wasteful [6]; the UID would eliminate corruption from the National Rural Employment Guarantee Scheme (NREGS) [6]; the UID would help ensure and monitor attendance of teachers in schools [7]. Overall, the UID project is presented as a "technology-based solution" that would change the face of governance in India.

3 Debating the Claims

If the conditions of life of its citizens are any indicator, India can safely be termed a backward economy and society. According to a survey of the government's National Sample Survey Organisation (NSSO) in 2004-05, about 77 per cent of India's population lived at an average monthly per capita consumption expenditure (MPCE) of Rs 16 per day (or 0.34 US $). The median number of years of schooling of an average Indian rural woman in 2005-06 was zero. More than 1 in 18 children in India died

within the first year of life, and 1 in 13 children died before reaching age 5 in 2005-06. Among children under age 3, about 38 per cent were stunted and about 46 per cent were underweight in 2005-06.

In sum, the extent of reach of basic social services to the Indian population is extremely poor. Indeed, the role of the state in transforming such backwardness in the life of its citizens is central. As such, the levels of expenditure of the state as well as efficient implementation of the state's welfare programmes have great instrumental value. Social scientists have long argued that the poor state of governance in India, particularly in areas like poverty alleviation, demands a closer look at the nature of the Indian state itself. In rural India, where majority of Indians live, the continuing concentration of political power in the hands of the landed elite is one of the fundamental barriers to improve the quality of governance. The lack of implementation of land reforms has aided the continued domination of these landed classes, also from the upper caste groups, and stymied democratization in the rural areas. According to John Harriss, "the structure and functioning of 'local agrarian power', and the relations of local and state-level power-holders, do exercise a significant influence on policy processes and development outcomes" in rural India (Harriss, 1995, p. 3376) [8].

It follows that any effort to comprehensively improve governance has to begin from the overhauling of local power structures and passing down political power to the under-privileged sections. Of course, advances in technology can be a major supplement to these efforts at democratizing the state and society. In certain spheres, technology can play a role in hastening change as well as reducing the drudgery of manual work. Further, a technology-based solution works best, and gives the most optimal results, when it is implemented in societies that are ready to absorb the technology. As Thomas and Parayil (2008, p. 431) argue with respect to governance, "social structures that tolerate illiteracy, landlessness and other inequities among large sections of the population deprive the individual of the capabilities to use ICTs and to benefit from the information that ICTs provide [9]." However, a perusal of the claims made in favour of the UID project in India would have us believe that the introduction of modern technology can help the state bypass fundamental reforms at social transformation.

I argue in this note that the UID project, while being presented as a tool of "good governance", would actually lead to the violation of a large number of freedoms of Indian people. No amount of assertion vis-à-vis improved service delivery can justify the violation of citizen's freedoms and liberties. Next, I argue that there is a misplaced emphasis on the benefits of technology in this project, when the robustness of that technology to handle large populations remains largely unproven. Further, I argue that no detailed cost-benefit analysis of the project has been carried out yet. Finally, I try to show, with an illustration, that the roots of inefficiency in public welfare schemes in India do not lie in the absence of identity proofs. In arguing all the above, I have used the literature on the experiences of more modern nations of the world in providing people with unique ID cards and numbers.

3.1 Privacy and Civil Liberties

International experience shows that very few countries have provided national ID cards or numbers to their citizens. The most important reason has been the unsettled

debate on the protection of privacy and civil liberties of people. It has been argued that the data collected as part of providing ID cards or numbers, and the information stored therein, may be misused for a variety of purposes. For instance, there is the problem of "functionality creep" where the card or number can serve purposes other than its original intent. Some have argued that ID cards or numbers can be used to profile citizens in a country and initiate a process of racial or ethnic cleansing, as during the genocide of Tutsis in Rwanda in 1995.[1] Legislations on privacy cannot be satisfactory guarantees against the possibilities of misuse of ID cards or numbers.

Learning from Western experiences. Chronologically, Australia was one of the first countries to try the implementation of a national ID card scheme in the recent years. In 1986, the Australian government introduced a Bill in the Parliament to legalise the issue of national ID cards, which were to be called as "Australia Cards". The declared intention of the government cited in the Bill was to check tax evasion as well as reduce illegal immigration. However, citizens' groups launched a major agitation against the Bill citing concerns of violation of privacy and civil liberties. Though the government tried hard to push the Bill, it had to finally withdraw the Bill in 1987.

Despite the failure to introduce the ID card scheme in Australia, other countries like Canada, New Zealand and Philippines initiated steps in the early-1990s to introduce national ID cards. In all these countries, the scheme had to be withdrawn after strong public backlash. In Canada, the Parliamentary Standing Committee on Citizenship and Immigration that examined the case for ID cards noted in its report that:

> It is clear that this is a very significant policy issue that could have wide implications for *privacy, security, and fiscal accountability*. Indeed, it has been suggested that it could affect fundamental values underlying Canadian society. A broad public review is therefore essential. The general public must be made more aware of all aspects of the issue, and we must hear what ordinary citizens have to say about the timeliness of a national identity card (cited in Davies, 2005; emphasis added) [10].

In the early 2000s, China declared its intention to introduce national ID cards along with biometric information. However, on an understanding that biometric technology is liable to major failures when applied to large populations as China's, the Chinese government in 2006 withdrew the clause to have biometric data stored in such cards.

Among many European nations, the nature of public sentiment has governed the form in which identity cards are constructed (see Davies, 2005). For instance, Sweden and Italy have extraordinary regulations regarding the use of data in citizens' registries. In Germany, collection of biometric information is not allowed. In France, the ID card is not mandatory for citizens. In Greece, after public protests, regulators were forced to remove details regarding religious faith, profession and residence from ID cards.

Two countries where the issue of national ID cards has been extensively debated are the US and the UK. In both these countries, the project has been shelved after massive public protests.

---

[1] See "National Identification System: Do We Need One?" Senate Economic Planning Office, Government of Philippines, December 2005.

In the US, privacy groups have long opposed ID cards; there was strong opposition also when the government tried to expand the use of the social security number in the 1970s and 1980s [10]. The disclosure of the social security number to private agencies had to be stopped in 1989 after public protests. A health security card project proposed by the Bill Clinton administration was set aside even after the government promised "full protection for privacy and confidentiality." Finally, the George Bush administration settled in 2005 for an indirect method of providing ID cards to US citizens. In what came to be called as a "de-facto ID system", the REAL ID Act made it mandatory for all US citizens to get their drivers' licenses re-issued, replacing old licenses. In the application form for re-issue, the Department of Homeland Security added new questions that became part of the database on driving license holders. As almost all citizens of US had a driving license, this became an informal electronic database of citizens. Nevertheless, these cards cannot be used in the US for any other requirement, such as in banks or airlines. The debate on the confidentiality of the data collected by the US government continues to be live even today [11].

The most interesting debate on the issue of national ID cards has been in the United Kingdom. With the introduction of the Identity Cards Bill of 2004, the Tony Blair government declared its intent to issue ID cards for all UK citizens. Public protests have forced the Labour government to shelve the policy till date. The debate in UK has mainly centred around the critical arguments in an important research report on the desirability of national ID cards prepared by the 'Information Systems and Innovations Group' at the London School of Economics (LSE). The LSE's report is worth reviewing here.[2]

The LSE report identified key areas of concern with the Blair government's plans, which included their high risk and likely high cost, as well as technological and human rights issues. The report noted that the government's proposals "are too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence." While accepting that preventing terrorism is the legitimate role of the state, the report expressed doubts on whether ID cards would prevent terror attacks through identity theft:

> …preventing identity theft may be better addressed by giving individuals greater control over the disclosure of their own personal information, while prevention of terrorism may be more effectively managed through strengthened border patrols and increased presence at borders, or allocating adequate resources for conventional police intelligence work… A card system such as the one proposed in the Bill may even lead to a greater incidence of identity fraud… In consequence, the National Identity Register may itself pose a far larger risk to the safety and security of UK citizens than any of the problems that it is intended to address.

In conclusion, the LSE report noted that

[2] For the web site of the Identity Project at LSE, see http://identityproject.lse.ac.uk. The full report is available at http://identityproject.lse.ac.uk/identityreport.pdf and the Executive Summary of the report is available at http://identityproject.lse.ac.uk/identitysummary.pdf

> …identity systems may create a range of new and unforeseen problems. These include the failure of systems, unforeseen financial costs, increased security threats and unacceptable imposition on citizens. The success of a national identity system depends on a sensitive, cautious and cooperative approach involving all key stakeholder groups including an independent and rolling risk assessment and a regular review of management practices. We are not confident that these conditions have been satisfied in the development of the Identity Cards Bill. The risk of failure in the current proposals is therefore magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals.

The Western debates reviewed here bring forth serious questions regarding the potential of national ID cards to subvert hard-won rights of people to privacy and civil liberties in the modern world. National debates in each of these countries have influenced the final outcomes in these schemes, and citizens have reacted collectively to the threats of intrusion into their basic democratic rights. In fact, in most of the few countries that have introduced national ID cards, the periods of introduction have also been of either an authoritarian government or a war.

Issues of Privacy and the UID Project in India. The UIDAI in India has declared that the UID would not confer citizenship on any individual and that enrolment into the scheme would not be mandatory. However, other pronouncements from the UIDAI have made it clear that the UID is likely to be used in a wide variety of welfare schemes. It is thus clear that even while there would not be a *de jure* insistence on the UID, citizens would *de facto* be forced to apply for UID to access many welfare schemes. Thus, "indirect compulsoriness" is a central feature of the UID project in India.

What is most disturbing in the Indian scenario is that the concerns of privacy or civil liberties are not discussed in any of the documents of the government or the UIDAI in any substantive form. It has been made to appear as if the purported, and unsubstantiated, benefits of 'good governance' from the project eclipse the concerns regarding human rights. Information that is available point to the possibilities of serious misuse of personal information if the UID is extended to a spectrum of social services, most of which are increasingly being privatized in India. Take an example: the UID project in India is being implemented as part of the eleventh five year plan of the government. In 2006, a working group was appointed by the Planning Commission to examine the possibilities and potential of an Integrated Smart Card System to improve the entitlements of the poor. In its report, the working group noted that the:

> …unique ID could form the fulcrum around which all other smart card applications and e-governance initiatives would revolve. This could also form the basis of a public-private-partnership wherein *unique ID based data can be outsourced to other users*, who would, in turn, build up their smart card based applications… (GoI, 2007, p. 2; emphasis added) [12].

> …In the context of the unique ID, part of this data base *could be shared with even purely private smart card initiatives such as private*

> *banking/financial services on a pay-as-you-use principle*…. (p. 8; emphasis added).
>
> These agencies [private utility services providers or financial and other institutions] can 'borrow' unique ID *and related information* from the managers of these data bases and load further applications in making requirement specific smart-cards. While the *original sources of data can be updated by the data managers*, the updating of supplementary parts will remain the responsibility of the service providers (p. 24; emphasis added).

Personal information of citizens is rendered all the more vulnerable to misuse in a policy atmosphere that explicitly encourages private participation in social service delivery. Citing the case of privacy of health records of citizens, an observer of the UIDAI noted recently that:

> …the Apollo Hospitals group has offered to manage health records through the UIDAI. It has already invested in a company called Health Highway that reportedly connects doctors, hospitals and pharmacies who would be able to communicate with each other and access health records. In August 2009, Business Standard reported that Apollo Hospitals had written to the UIDAI and to the Knowledge Commission to link the UID number with health profiles of those provided the ID number, and offered to manage the health records. The terms 'security' and 'privacy' seem to be under threat, where technological possibility is dislocating many traditional concerns (Ramanathan, 2010) [13].

At present, the UIDAI has only affirmed a commitment to protection of privacy; no substantial information is yet available on how the database of citizens would be protected from misuse in the future. As I argued earlier, promises to introduce privacy-protection legislations are poor tools to gain the trust of citizens, who face real threats of misuse of personal information.

3.2 Technological Determinism in Addressing Social Problems

An interesting aspect of the discussion on the UID project in India has been the level of technological determinism on display. The fact that the UIDAI is headed by a technocrat like Nandan Nilekani, and not a demographer or any social scientist, is evidence to the technological bias in the project. The problems of enumeration in a society like India's, marked by illegal immigration as well as internal migration, especially of people from poor labour households, are too enormous to be handled effectively by a technocrat. It is intriguing that the duties of the Census Registrar and the UIDAI Chairman have been demarcated, and that the UIDAI Chairman has been placed in the rank of a Cabinet Minister above the Census Registrar.

Among all the technological features of the UID project, it is the collection and storage of biometric information of residents that is most significant. The UIDAI plans to collect a basic set of personal information from all residents and store them in a centralised database along with their biometric information, such as finger prints of

all the 10 fingers in the hands as well as iris scans. Users of this massive centralized database would be public and private service providers; for purposes of verification, all service providers would have access to the centralised database. Biometric data would be used to verify the identity of the person whenever a UID-compliant service is provided. In other words, machines that verify the biometric data of the citizens would be installed at all the sites of service provision. Access to the service would be dependent on a positive verification of the biometric information.

For a country with more than a billion residents, the sheer scale of the envisaged project is mind-boggling. As per estimates, there are about half a million public food distribution outlets in India; there are about 265,000 gram panchayats (decentralised local bodies of governance) through which social service provision is managed. This is apart from millions of other offices of the government and public institutions that take part in the process of everyday governance. In other words, the crucial question is: can the technological infrastructure of the project carry the burden of such massive data storage, networking, live sharing and verification? If so, what are the associated costs of the project (see next section)? What are the probabilities of system failures of different degrees? What are the probabilities of errors? What are the "social" costs of these errors? No clear answers are available for these important questions.

The use of biometrics. The use of biometrics is the central feature of the UID project; apart from biometrics, there is no valid identity check in the system. There appears to be an extraordinary level of faith among the proponents of the project in the infallibility of biometric verification. On the other hand, there is consensus among biometric scientists and legal experts regarding critical drawbacks of the technology in proving identity beyond doubt.

First, many biometric and legal experts have argued that no accurate information exists on whether the errors of matching fingerprints are negligible or non-existent (see Koehler, 2008) [14]. It is acknowledged that a small percentage of users would always be either falsely matched or not matched at all against the data base. Fears have also been raised on the different ways in which users could bypass the verification process by using methods like "gummy fingers" and "latent finger printing." In other words, a completely new identity, different from the original, could be created and used consistently over a period of time.

Secondly, the concern remains if biometric information collected as part of the UID project would be used for policing purposes. In what is a typical case of "functionality creep", police and security forces, if allowed access into the biometric data base, could extensively use it for regular surveillance and investigative purposes. One, regular use of biometric data in policing can lead to a large number of human rights violations. Two, coupled with the possibility of errors in fingerprint matching, the use of biometric data in policing can further aggravate the extent and depth of human rights violations.

For instance, a recent concern in the legal circles in the US is whether validation checks of fingerprints are conclusive or not (see Cole, 2006) [15]. Increasing number of prison detentions in the US based on false fingerprint matches are cited as evidence for the possible human rights violations that could result. In 2004, the *New Scientist* ran an investigative story titled "Forensic Evidence in the Dock" [16]. The authors argued that "supposed infallibility of fingerprint evidence, which has been used to convict countless people over the past century" was still routinely accepted by US

courts. In 1999, a US court agreed to hold a "Daubert hearing" over a case of robbery registered against Byron Mitchell, whose finger prints "matched" the finger prints recorded from the site of the crime. A Daubert hearing is a special hearing where the judges take a decision on the scientific validity and reliability of any forensic evidence before it is submitted. While taking a decision on the Daubert hearing, the judges have to judge the defined error rate of the forensic evidence submitted. It turned out that no study on error rates existed. The court then asked the FBI to conduct a study, whose results have been argued to be methodologically erroneous by many legal observers [16]. The debate on the validation of fingerprints is as yet unsettled within the US legal system.

For purposes of illustration, I shall cite two instances from Cole (2005, pp. 986-987) [17] of false matching of finger prints in the US that led to massive protests from human rights activists:

> …the case of Brandon Mayfield, an Oregon attorney and Muslim convert who was held for two weeks as a material witness in the Madrid bombing of March 11, 2004…Mayfield, who claimed not to have left the United States in ten years and did not have a passport, was implicated in this attack almost solely on the basis of a latent fingerprint found on a bag in Madrid containing detonators and explosives in the aftermath of the bombing. Unable to identify the source of the print, the Spanish National Police emailed it to other police agencies. Federal Bureau of Investigation (FBI) Senior Fingerprint Examiner Terry Green identified Mayfield as the source of the latent print. Mayfield's print was in the database because of a 1984 arrest for burglary and because of his military service. The government's affidavit stated that Green "considers the match to be a 100% identification" of Mayfield…
>
> …A few weeks later the FBI retracted the identification altogether and issued a rare apology to Mayfield. The Spanish National Police had attributed the latent print to Ouhnane Daoud, an Algerian national living in Spain…
>
> …But the Mayfield case was not the first high-profile fingerprint misattribution to be exposed in 2004. In January, Stephan Cowans was freed after serving six and a half years of a 30- to 45-year sentence for shooting and wounding a police officer. Cowans had been convicted solely on fingerprint and eyewitness evidence, but post-conviction DNA testing showed that Cowans was not the perpetrator. The Boston Police Department then admitted that the fingerprint evidence was erroneous, making Cowans the first person to be convicted by fingerprint evidence and exonerated by DNA evidence.

Thirdly, the UIDAI has noted that it plans to introduce the project in a set of flagship schemes of the government, including the National Rural Employment Guarantee Scheme (NREGS). In other words, the access to this important employment scheme for rural labourers in India would be made completely dependent on biometric verification. It is estimated that there are more than 30 million persons in India who possess "job cards" (or, are beneficiaries) of NREGS.

A fundamental issue that biometric experts do not dismiss away is the possibility of fingerprints of individuals changing over time, particularly among manual labourers. Given the heavy manual labour that rural poor are regularly involved in (apart from cases of accidental damage to fingers and hands from burns, chemicals, and other agents), the fingerprints of manual labourers are highly likely to be broken or get eroded, inviting frequent negative responses during validation at the sites of wage payments. Globally, about 2 to 5 per cent of the population is held to have noisy or bad data on finger prints; in other words, their finger prints are permanently damaged to the extent that they can not be recorded in the first place [18]. According to some estimates, in developing countries like India, the share of persons with noisy or bad data could go up to 15 per cent, given the larger share of population dependent of hard manual labour [19]. In a country with a population of more than one billion people, a 15 per cent share would mean a minimum of 150 million persons. That is likely to be a rough count of the extent of exclusion in welfare schemes due to the UID project.

The report of the UIDAI's internal Biometrics Standards Committee actually accepts these concerns as real. In its report, the Committee recognises that "a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts" (UIDAI, 2009b, p. 4). It has further noted that it is:

> …conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context (UIDAI, 2009b, p. 4) [20]

Yet, the UIDAI Chairman Nandan Nilekani declared in November 2009 that he planned to "issue the first UID number in next 12-18 months and cover 600 million in the next five and half years."[3]

The case of UK. Technological determinism has been a feature of efforts to introduce ID cards in other countries too, such as the UK. The rhetorical confidence of the UK government in the scheme has always sat uncomfortably with its own technological uncertainty regarding the project. Critics pointed out that a slight failure in any of the technological components may immediately affect underlying confidence of people in the scheme as a whole. For instance, the LSE report noted that:

> The technology envisioned for this scheme is, to a large extent, untested and unreliable. No scheme on this scale has been undertaken anywhere in the world. Smaller and less ambitious systems have encountered substantial technological and operational problems that are likely to be amplified in a large-scale, national system. The proposed system unnecessarily introduces,

[3] See Interview with Nandan Nilekani (2009), "We'll use best biometric, storage & search solns", available at http://igovernment.in/site/Well-use-best-biometric-storage--search-solns

> at a national level, a new tier of technological and organisational infrastructure that will carry associated risks of failure. A fully integrated national system of this complexity and importance will be technologically precarious and could itself become a target for attacks by terrorists or others.

3.3 The Unknown Costs of the UID Project

The costs involved in a project of the size and scale as the UID project are always enormous and have to be weighed against the limited benefits that are likely to follow. The estimated costs of implementing the project have not yet been disclosed by the government, while media reports indicate varying figures. According to information that has trickled out of the Planning Commission, the estimated initial cost of the project would be anywhere above Rs 20,000 crores (or about 4,348 million US $). Even after the commitment of such levels of expenditures, the uncertainty over the technological options and ultimate viability of the scheme remains. Nandan Nilekani himself noted in November 2009 that "no exact estimation of the savings can be made at this juncture".[4] In addition, it is unclear whether recurring costs for maintaining a networked system necessary for UID to function effectively have been accounted for by the government.

In the case of UK, the LSE report had noted that the costs of the scheme were significantly underestimated by the UK government. The critique of the LSE group on the costing exercise of the UK government is a good case study of why the costs of such schemes are typically underestimated. The LSE group estimated that the costs would lie between £10.6 billion and £19.2 billion, excluding public or private sector integration costs. This was considerably higher than the estimate of the UK government.

3.4 The Efficiency of Social Sector Schemes

Would the UID result in an increase in the efficiency of government's poverty alleviation schemes? According to the Chairman of UIDAI, the UID "will help address the widespread embezzlement that affects subsidies and poverty alleviation programmes [21]." This conviction comes from a basic diagnosis of the UIDAI: that the inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies.

However, it is difficult to foresee any major shift in the efficiency frontiers of poverty alleviation programmes once UID is introduced. The reason is that the premise of the claim made by the UIDAI (that proven identities would expand access to schemes) is in itself erroneous. The poor efficiency of government schemes in India is not due to the absence of technological monitoring. The reasons are structural, and these structural barriers cannot be transcended by using a UID. I shall illustrate this using the example of one important social sector scheme: the public distribution system (PDS) that supplies subsidized food grains to the people.

---

[4] Ibid.

The case of the PDS. In the 1990s and 2000s, economic policy in India took a major shift towards neo-liberal policies. Till 1996-97, the PDS in India was universal in character. In other words, all households who owned a ration card were eligible to purchase commodities at subsidised prices. Under the neo-liberal policy regime, PDS ceased to be universal in character. Instead, a Targeted Public Distribution System (TPDS) was introduced where all households were divided into two categories: Below Poverty Line (BPL) and Above Poverty Line (APL) households. Only those households classified as BPL were eligible for the subsidised purchase of commodities. Such a shift towards targeting is not specific to India; globally itself targeting is the most important instrument used under the policy of structural adjustment in the provision of social security assistance. Targeting reduces the burden that the state has to bear with respect to social assistance by narrowing down the "eligible" proportion of the population to a minimum.

The introduction of the TPDS has led to major issues in the functioning of the food distribution system. A widespread complaint from rural India after the introduction of TPDS has been the existence of a major mismatch between households classified as BPL by the government and their actual standard of living (Swaminathan 2000 [22]; Swaminathan and Misra 2002 [23]; GoI 2002 [24]). A high-level committee appointed by the government in 2002 concluded that 'the narrow targeting of the PDS based on absolute income-poverty is likely to have excluded a large part of the nutritionally vulnerable population from the PDS" (GOI 2002) [24]. In other words, the poor "efficiency" of the PDS and its absence of reach has been a policy-induced phenomenon under the neo-liberal regime.

While the real reason for the inefficiency of the PDS in India is the policy of narrow targeting, the claim of the UIDAI has been that the UID would plug leakages in the functioning of the PDS. In other words, the UID would ensure that targeting is as accurate as possible, and no "ineligible" person buys subsidized food grains from the PDS. In simple terms, this is inverted logic.

The most important problem with the PDS in India is not that non-BPL households benefit, but that large sections are not classified as BPL in the first place. Further, there are major problems associated with having a classification of households as BPL or APL based on a survey conducted in one year, and then following the same classification for many years. Incomes of rural households, especially rural labour households, fluctuate considerably. A household may be non-poor in the year of survey, but may become poor the next year due to uncertainties in the labour market. How would UID solve this most important barrier to efficiency in the PDS? While the real challenge in PDS is to expand the coverage to newer sections of the population, the UID has been showcased as an intervention that would actually make it as narrowly targeted as possible.

Yet another claim is that a simple cash-transfer scheme would become possible if a UID is introduced, which could replace the existing poverty alleviation programmes. To begin with, cash-transfer schemes have not been found to be efficient substitutes for public works schemes in any part of the developing world. In addition, for the same reasons discussed in the context of the PDS, a cash-transfer scheme would also lead to the exclusion of a large number of needy from cash benefits. A UID cannot be of any help in such scenarios.

4 Concluding Notes

In conclusion, the UID project of the Indian government appears to be missing the grade on most criteria. There is no reason to discount the concern that a centralized database of citizens' personal and biometric information could be misused to profile citizens in undesirable and dangerous ways. There is an unrealistic assumption behind the project that technology can be used to fix the ills of social inefficiencies. The benefits from the project, in terms of raising the efficiency of government schemes, appear to be limited. Given available information, the scheme appears to be extraordinarily expensive, without concomitant benefits.

This is not to argue against any form of electronic management of data or provision of services, including a regulated and sector-specific use of biometrics. For instance, when the intended beneficiary populations are smaller – as, for instance, in an old age pension scheme – such an initiative may function better than on a massive scale as to one billion people.

The central issue with the UIDAI initiative is that technology is thought of as a short cut to bypass difficult and more fundamental societal changes. On the other hand, the lessons from history are that there are no short cuts to progressive social change. The worldview that drives the UIDAI, unfortunately, is the former.

References

1. Friedman, T.L.: The World is Flat: A Brief History of the Twenty-First Century. Farrar, Strauss and Giroux, New York (2005)
2. Taha, M.: Notes from a Contested History of National Identity Card in India: 1999-2007 (accessed January 28, 2008), http://www.sacw.net/article391.html
3. Ministry of Home Affairs Notification (December 10, 2003), http://www.censusindia.gov.in/Acts_and_Rules/citizenship_rules_2003.pdf (accessed February 9, 2010)
4. Press Release of the Press Information Bureau, Government of India., http://pib.nic.in/release/release.asp?relid=44711 (accessed January 28, 2010)
5. Dhoot, V.: Unique ID cards will make bank account, phone connection easy. Financial Express. (2009), http://www.financialexpress.com/news/unique-id-cards-will-make-bank-account-phone-connection-easy/529183 (accessed January 28, 2010)
6. UIDAI, Creating a Unique Identity Number for Every Resident in India, working paper. Unique Identification Authority of India, New Delhi (2009)
7. Unique ID number for checking absenteeism of teachers?. Press Trust of India, New Delhi. http://www.ptinews.com/news/470034_Unique-ID-number-for-checking-absenteeism-of-teachers (accessed February 9, 2010)
8. John, H.: Comparing Political Regimes across Indian States: A Preliminary Essay. Economic and Political Weekly 34(48), 3367–3377 (1999)
9. Thomas, J.J., Parayil, G.: Bridging the Social and Digital Divides in Andhra Pradesh and Kerala: A Capabilities Approach. Development and Change 39(3), 409–435 (2008)
10. Davies, S.: The Complete ID Primer. Index on Censorship 3 (2005), http://www.eurozine.com

11. For a useful set of questions and answers on the national ID scheme in the US, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61881 (accessed January 28, 2010)
12. Government of India, Entitlement Reform for Empowering the Poor: The Integrated Smart Card (ISC). Report of the Eleventh Plan Working Group on Integrated Smart Card System, Planning Commission, New Delhi (2007)
13. Usha, R.: The Personal is the Personal. Indian Express (2010), http://www.indianexpress.com/news/the-personal-is-the-personal/563920/0 (accessed January 28, 2010)
14. Koehler, J.J.: Fingerprint Error Rates and Proficiency Tests: What they are and Why they Matter. Hastings Law Journal 59(5), 1077–1100 (2008)
15. Cole Simon, A.: Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents Discourse. Law and Policy 28(1), 109–135 (2006)
16. Randerson, J., Coghlan, A.: Investigation: Forensic evidence in the dock. New Scientist (2004), http://www.newscientist.com/article/dn4611-investigation-forensic-evidence-in-the-dock.html (accessed January 28, 2010)
17. Cole, S.A.: More than Zero: Accounting for Error in Latent Fingerprint Identification. The Journal of Criminal Law & Criminology 95(3), 985–1078 (2005)
18. Jain, A.K., Dass, S.C., Nandakumar, K.: Can Soft Biometric Traits Assist in User Recognition? Proceedings of SPIE 54(4), 562 (2004)
19. De-duplication: The Complexity in the Unique ID Context. 4G Identity Solutions, http://www.4gid.com/De-dup-complexity%20unique%20ID%20context.pdf (accessed January 28, 2010)
20. UIDAI, Biometric Design Standards for UID Applications. Report of the UID Committee on Biometrics, Unique Identification Authority of India, New Delhi (2009)
21. Ramakumar, R.: High-cost, High-risk. Frontline, 26 (15). (2009), http://www.hinduonnet.com/fline/fl2616/stories/20090814261604900.htm (accessed January 28, 2010)
22. Swaminathan, M.: Weakening Welfare: The Public Distribution of Food in India. Left-Word Books, New Delhi (2000)
23. Swaminathan, M., Misra, N.: Errors in Targeting: Public Food Distribution in a Maharashtra Village, 1995-2000. Economic and Political Weekly, 2447–2450 (2002)
24. Government of India (GoI), High Level Committee on Long-Term Grain Policy. Ministry of Food and Public Distribution, Government of India, New Delhi (2002)