

# UID

tracking, profiling and surveillance of citizens

Campaign for NO UID

15th August 2010

Published for education in public interest  
by  
Campaign for NO UID  
c/o. INSAF  
A124/6,  
Katwaria Sarai,  
New Delhi 110016

15th August 2010

NOT FOR SALE

Printed by:  
Design & Dimensions  
New Delhi (9810686122)

# THE PERSONAL IS THE PERSONAL

---

USHA RAMANATHAN IN THE INDIAN EXPRESS

---

THE air is thick with schemes that will enable the state, and its agencies, to identify every resident, and to track what they are doing. A home ministry project for creating a National Population Register which will be prepared along with the 2011 Census has been propelled through its pilot stage. Now, an ambitious programme has been launched to load all the residents of the country on to a data base, providing each of us with a unique identity number. What distinguishes this exercise from any other undertaken so far?

First of all, the intention is provide a Unique Identity Number to the whole population, including the just born. The state is to have data on each individual literally from birth to death; and beyond, for a person's UID is not destroyed at death, merely disabled. The numbers are to be so generated that it will not have to be repeated for between a hundred and two hundred years.

The UIDAI, in its working paper, says that enrolment will not be mandatory, but acknowledges that in practice it is expected not

to be voluntary. The 'Registrars', who will enroll people on to the data base, will be both private operators and government agencies, and they will be encouraged to insist that they will entertain only those who are willing to enroll. Over a short time, only those with UID numbers may find themselves able to access services. That is the effort.

The UID has nothing to do with citizenship. The information on the UID database is expected to be basic, and to cover all residents: name, date of birth, place of birth, gender, the name and UID numbers of both parents, address, date of death and photograph and fingerprints. This is because the UID is only to identify the individual to the agency that is looking for authentication.

**JUST ON ITS OWN, IT COULD EVEN SEEM BENIGN.**

There are two phenomena that take the innocence out of the exercise. The first is 'convergence'. 'Convergence' is about combining information. 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 passport agencies do not need to know how many bank accounts you have, or whether you drive a car. The telephone company need not know how you have insured your house. The police do not need to know how often you travel, not unless you are a suspect anyway. It is this that makes some privacy possible in a world where there are so many reasons why, and locations where, we give information about ourselves. 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.

This is poised to completely change norms of privacy, confi-

dentiality and security of personal information. There are already indications about how convergence will work. Consider the reports 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.

The second phenomenon is 'tracking'. Once the UID is in place, and convergence becomes commonplace, the movement of people, their monies, their activities can be brought together, especially since transactions from buying rice in a PDS shop to receiving wages to bank withdrawals to travel could begin to require the number. There is a difference between people tracking a state, and the state, and the 'market' tracking people. The UID is clearly not what it is presented as being: it is not benign, nor a mere number which will give an identity to those who the state had missed so far.

Interestingly, the working paper of the UIDAI starts with a claim that the UID will bring down barriers that prevents the poor from accessing services and subsidies by providing an identity, but soon goes on to clarify that the "UID number will only guarantee identity, not rights, benefits or entitlements". Given that it is the powerlessness of the poor, inefficiency, the perception of the poor as not deserving of support, sympathy or rights, and the status of illegality foisted on them that stops them from getting what is due to them, and given that corruption and leakages in the system mutate and persist, this quick stepping back is wise indeed.

In the excitement about technology being deployed to do something that has not been done anywhere in the world, the importance of privacy and protection from misuse of personal information is getting eclipsed.

It is significant that the UIDAI working paper makes no mention of national security concerns, and the surveillance, and profiling, possibilities it will create. Yet, the UID is not a project in isolation. The NATGRID, which the UID will facilitate, places the whole population under surveillance; and the home minister is talking about a DNA bank.

Fallibility, the difficulties inherent in reaching those in extreme poverty, the choiceless existence on a database and the possibility of undesirable others getting hold of information only add to the scariness of the scenario that we seem to have accepted without discussion, challenge or debate. And, once accomplished, we would have reached a point of no return.

The writer is an independent law researcher.

*<http://www.indianexpress.com/news/the-personal-is-the-personal/563920/0>*

*Vol:26 Iss:16 URL: <http://www.flonnet.com/fl2616/stories/20090814261604900.htm>*

# HIGH-COST, HIGH-RISK

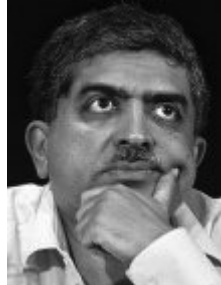
---

R. RAMAKUMAR

---

*The UPA government is going ahead with the ID card project, ignoring criticisms and alternative suggestions.*

*Nandan Nilekani, Chairperson, Unique Identification Authority.*



WITH the appointment of Nandan Nilekani as the Chairperson of the Unique Identification Authority (UIA), it is clear that the United Progressive Alliance (UPA) government has decided to go ahead with the controversial project to provide each Indian citizen with a unique and multi-purpose identity card. The media are abuzz with commentators praising the government for a landmark decision that would "change the face of governance" in India. With contracts worth hundreds of crores up for grabs, the IT industry too is in delight. "Bring them on! We will fix it," the tech industry appears to be claiming on what is essentially a social problem.

The project was initiated by the National Democratic Alliance government under Atal Bihari Vajpayee in 2002. A perusal of its history shows that the dirty groundwork had already been completed under the NDA. The origins of the project can be traced back to the controversial report of the Kargil Review Committee, appointed in the wake of the Kargil War, in 1999. This committee was chaired by K. Subrahmanyam and had as its members B.G. Verghese, Satish Chandra and K.K. Hazari. In its report submitted in January 2000, the committee noted that immediate steps were needed to issue ID cards to villagers in border districts, pending its extension to other parts of the country. By around 2001, a Group of Ministers of the NDA government submitted a report to the government, titled Reforming the National Security System. This report was based largely on the findings of the Subrahmanyam Committee. The report noted:

"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, which was to form the basis for the preparation of ID cards. The best way was to link the preparation of the register with the Census of India. However, the Census has always had strong clauses relating 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 the 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 December 10, 2003, the onus for registration was placed on the citizen: "It shall be compulsory for every Citizen of India to...get himself registered in the Local Register of Indian Citizens." The rules also specified punishments for citizens who failed to do so; any violation was to be "punishable with fine, which may extend to one thousand rupees".

In other words, the privacy clauses relating to Census surveys were diluted significantly by the NDA government in 2003 itself.

The UPA government has only carried forward the plans of the NDA government under a new name. The MNIC project was replaced by the National Authority for Unique Identity (NAUID), and placed under the Planning Commission. The NAUID was established in January 2009, after the terrorist attacks on Mumbai in November 2008. However, the steps to establish it had begun even before the Mumbai attacks.

According to a press release of the government dated November 10, 2008, the Unique Identity (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." 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." As per the interim budget of the UPA government in February 2009, the UIA was established.

The public response to the ID project has been influenced by the liberal praise that the media have showered on it. In fact, the nature of reporting would have one in doubt on whether the praise is for the project per se or for the appointment of the Chairperson. Some commentators hailed Nilekani's appointment

as a first step in the absorption of technocrats into government. It has also been argued that ID cards would increase the efficiency of poverty alleviation programmes. In fact, while better delivery of poverty alleviation programmes is the stated primary objective of the project, it is no one's doubt that the actual primary objective is to address terrorism.

Indeed, the presence of identity cards for citizens in an electronic format is a welcome measure. In specific sectors/schemes and in specific contexts, it can increase the efficiency of service delivery. At the same time, there are a number of reasons why the UIA project has to be thoroughly critiqued, and even opposed.

#### **PRIVACY & CIVIL LIBERTIES**

First, international experience shows that very few countries have provided national ID cards to citizens. The most important reason has been the unsettled debate on the protection of privacy and civil liberties. It has been argued that the data collected as part of providing ID cards, and the information stored in the cards, may be misused for a variety of purposes. For instance, there is the problem of "functionality creep" where the card can serve purposes other than its original intent. Some have argued that ID cards can be used to profile citizens in a country and initiate a process of racial/ethnic cleansing, as during the Rwanda genocide of 1995. Legislation on privacy cannot be a guarantee against the possibilities of misuse of ID cards.

Two countries where the issue of national ID cards has been well debated are the United States and the United Kingdom. In both these countries, the project was shelved after public protests. Countries such as Australia have also shelved ID card schemes. While China declared its intention to introduce an ID card, it later withdrew the clause to have biometric data stored in such cards.

In the U.S., privacy groups have long opposed ID cards; there was opposition also when the government tried to expand the use of the social security number in the 1970s and 1980s. The disclosure of the social security number to private agencies had to be stopped in 1989 following a public outcry. A health security card project proposed by Bill Clinton was set aside even after the government promised "full protection for privacy and confidentiality".

Finally, the George W. Bush administration settled in 2005 for an indirect method of providing ID cards to U.S. citizens. In what came to be called a "de-facto ID system", the REAL ID Act made it mandatory for all U.S. citizens to get their drivers' licences re-issued, replacing old licences. In the application form for reissue, the Department of Homeland Security added new questions that became part of the database on driving licence holders. As almost all citizens of the U.S. had a driving licence, this became an informal electronic database of citizens. Nevertheless, these cards cannot be used in the U.S. for any other requirement, such as in banks or airlines. The debate on the confidentiality of the data collected by the U.S. government continues to be alive even today.

The most interesting debate on the issue of national ID cards has been in the U.K. With the introduction of the Identity Cards Bill of 2004, the Tony Blair government declared its intent to issue ID cards for all U.K. citizens. Public protests have forced the Labour government to shelve the policy to date. The debate 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.

#### **LSE's REPORT**

The 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 U.K. citizens than any of the problems that it is intended to address."

In conclusion, the LSE report noted that "...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."

#### **TECHNOLOGICAL DETERMINISM**

Secondly, an interesting aspect of the discussion in India is the level of technological determinism on display. It would appear that the

problem of citizenship can be fixed by the use of technology. The fact that the UIA is to be headed by a technocrat like Nilekani, and not a demographer, is evidence to this biased view of the government. 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 UIA Chairperson have been demarcated, and that the UIA Chairperson has been placed as a Cabinet Minister above the Census Registrar.

Such technological determinism has been a feature of efforts to introduce ID cards in other countries too, such as the U.K. The rhetorical confidence of the U.K. 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:

*Shiv Kumar Chinna Coundar in Mumbai with a temporary ID card issued by a fishermen's society that allows him to work while waiting for a state-issued ID card, which became compulsory for all fishermen on the open seas after*



*the November 2008 terror attack on Mumbai. The origins of the ID card project can be traced to the Kargil Review Committee report, which noted that immediate steps were needed to issue*

*ID cards to villagers in border districts, pending its extension to other parts of the country.*

"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, 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."

Blair, nevertheless, was an ardent advocate of the ID card scheme. In an article in *The Daily Telegraph*, he argued that ID cards were required to secure U.K's borders and ease modern life, and that "the case for ID cards is a case not about liberty but about the modern world". Responding to the invocation of modernity, Edgar A. Whitley, Reader at LSE and a member of its research team, noted that "intellectually, technological determinism seemed to us to reduce the intimate intertwining of society and technology to a simple cause-and-effect sequence."

Thirdly, would the ID card scheme result in an increase in the efficiency of the government's poverty alleviation schemes? According to Nilekani, the ID card "will help address the widespread embezzlement that affects subsidies and poverty alleviation programmes". However, it is difficult to foresee any major shift in the efficiency frontiers of poverty alleviation programmes if ID cards are introduced. The poor efficiency of government schemes in India is not because of the absence of technological monitoring. The reasons are structural, and these structural bar-

riers cannot be transcended by using ID cards.

### **COMPREHENDING SOCIAL REALITIES**

Take one claim - unique ID cards would lead to "better targeting of government's development schemes". Here is where the thinking behind the ID cards fails to comprehend the social realities that reduce the access of needy sections to welfare schemes. If we apply the argument to the Public Distribution System (PDS), it would imply that the government could ensure that only BPL households benefit from the scheme. But the most important problem with the PDS in India is not that non-BPL households benefit from it 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 because of uncertainties in the labour market. How will an ID card solve this most important barrier to efficiency in the PDS?

Yet another claim is that a simple cash-transfer scheme, which can replace existing poverty alleviation programmes, will become possible if ID cards are introduced. 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. An ID card cannot be of any help in such scenarios.

Also, the case of BPL cards cited above cannot be considered as a special case. Given that the BPL population has special privileges in many social welfare provisions, this would also be a larger and persistent problem in the use of ID cards for any purpose in the social sector.

Fourthly, the costs involved in such a project are always enormous and have to be weighed against the limited benefits that are likely to follow. In India, the cost estimated by the government itself is a whopping Rs.1.5 lakh crore. Even after the commitment of such levels of expenditures, the uncertainty over the technological options and ultimate viability of the scheme remains. In addition, it is unclear whether recurring costs for maintaining a networked system necessary for ID cards to function effectively have been accounted for by the government.

In the case of the U.K., the LSE report noted that the costs of the scheme were significantly underestimated by the government. The critique of the LSE group on the costing exercise of the U.K. 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 U.K. government.

Apart from the reasons discussed above, there are other simple questions for which answers are not easily forthcoming. Suppose a poor household, which has been regularly using the ID card, loses the card. Would that mean that all the benefits to the household will cease until a new card is provided (that is surely to take many weeks in the Indian context)? Why cannot we think of other options, such as providing separate electronic cards for some of the very important schemes? What happens to the use of ID cards in villages that do not even have electricity, leave alone Internet connections?



### **MISUSE OF DATABASE**

In conclusion, the ID card project of the UPA government, which is the continuation of a hawkish idea of the NDA, appears to be missing the grade on most criteria. There is no reason to disbelieve the argument that the centralised database of citizens could be misused to profile citizens in undesirable and dangerous ways.

The scheme is extraordinarily expensive. 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.

This is not to argue against any form of electronic management of data or provision of services. It may certainly be useful to have an identity card for citizens, which can be made use of in any part of the country for identification as well as for availing themselves of certain minimum benefits. At present, roughly 80 per cent of India's citizens have an election ID card. The use of this ID card can be easily expanded, with some innovation, to convert it into a master card for a specified set of purposes.

But what is the social benefit of centralising all information and access to welfare schemes into one smart card? Unfortunately, the UPA government has skipped public debate around criticisms and alternative suggestions. o

*R. Ramakumar is with the Tata Institute of Social Sciences, Mumbai.*

*Vol:27 Iss:12 URL: <http://www.flonnet.com/fl2712/stories/20100618271209400.htm>*

# QUESTIONABLE LINK

---

PRAFUL BIDWAI

---



*The UIDAI's plan to use population information compiled from Census 2011 data to generate the UID is fraught with dangers to individual freedoms and rights.*

– V. RAJU

The pilot project of the UIDAI involved collection of biometric data of individuals, including (above) iris information and (below) fingerprints and photographs in various places.

When the Unique Identification Authority of India (UIDAI) was launched last year, there was no debate on its purpose or clarity about what methods it would use to give each one of 1.2 billion Indians a 16-digit unique identity (UID) number.

Although its Chairman, Information Technology (IT) star Nandan Nilekani, was given Cabinet rank, the UIDAI was not placed under a Ministry but within the Planning Commission, a non-statutory body, which has increasingly appropriated power without public accountability. There was no discussion on the merits of the project vis-a-vis other means of identification for purposes such as employment guarantee schemes, below-poverty-line (BPL) cards, or education entitlements.

The project has since ballooned into a gargantuan scheme. The latest Budget raised its annual allocation 16-fold. It has a new name (Aadhaar) and a logo. Meanwhile, Nilekani has decided that biometric data, including scans of both irises and all 10 fingerprints, will be used for each individual's UID. Even children between five and 15 years will be included "in view of the Right to Education".

#### **NAGARA GOPAL**

The project is now riding piggyback on the Census-2011 enumeration, which has begun. The Census data will be used to prepare a National Population Register, which will compile detailed information on each individual under 15 heads, including name, sex,



date of birth, parents' details, present and permanent address, marital status and "if ever married, name of spouse". It will include biometric data. According to Nilekani, the UIDAI will act as "the back-office of the NPR" by "de-duplicating" the collected data to generate the UID. As we see below, the UID-NPR-Census link is illegitimate.

There is no clarity about the project's purpose and the legitima-

cy of one of its principal functions: profiling citizens from whom the state is potentially at risk, to fight terrorism.

All manner of claims are made about its virtues and its potential to contribute to governance: it will create a reliable register of citizens; demarcate genuine nationals from illegal migrants; help the state keep an eye on terrorists, tax dodgers and money-launderers; bring 60 per cent of the poor who do not have bank accounts into the banking system; and promote microcredit delivery through fingerprint-compatible mobile phones. Above all, the project is supposed to enable accurate targeting of health care, food, National Rural Employment Guarantee Act benefits to the poor, while eliminating leaks and reducing corruption.



**DIBYANGSHU  
SARKAR/AFP**

Confusion reigns on whether the UID will be mandatory or voluntary. Nilekani insists it will be optional and concedes that legitimate claimants will be excluded from benefits if it is made mandatory. Yet, log-

ically, its coverage must be comprehensive in order to be efficacious.

Many government functionaries see the UID as a technological fix to social and administrative problems, including leaks in service delivery. Nilekani is more ambivalent. He recently said: "It's early days to say how leakages can be plugged. We are working on it." The first set of UIDs will be issued between August 2010 and February 2011. By 2014, they will cover half the population, with 95 per cent accuracy.

**Security rationale**

The UID project looks like a solution in search of problems. It is sought to be justified through social and pro-poor functions that are well beyond its core-purpose and can perhaps be achieved by equally efficient means.

Its core rationale and primary purpose is much less lofty than its extravagantly claimed social benefits. It lies in security, surveillance and control - traceable to the idea of a mandatory Multipurpose National Identity Card for all Indians recommended by the Kargil Review Committee chaired by security hawk K. Subrahmanyam.

This committee greatly exceeded its brief and strayed into areas such as security and nuclear weapons doctrines. It seized the Kargil issue to drive a much larger "National Security State" agenda. Home Minister P. Chidambaram himself underscored the UID's security rationale by announcing the UIDAI's establishment in January 2009 as a timely response to the November 2008 Mumbai terror attacks.

This rationale further unfolded with the government announcing a plan to set up a DNA databank and a NATGRID (National Intelligence Grid) connecting 11 agencies, including the Intelligence Bureau, the Research and Analysis Wing, the Central Bureau of Investigation, the Directorate of Revenue Intelligence, the Central Board of Excise and Customs and the Central Board of Direct Taxes.

**Pivotal intermediary**

The information generated by the NPR will be shared with the UIDAI and NATGRID. The DNA bank and NATGRID are meant to combat terrorism and other challenges to internal security. The UIDAI will be a pivotal intermediary between numerous agencies: the Registrar General (which conducts the Census), the Reserve

Bank of India (which regulates commercial banks), and telephone and Internet providers, besides intelligence agencies. This is essential if the UID number is to be accepted as a proof of identity. But how reliable is the UID as the prime, if not sole, information base for security agencies, indeed even the civilian administration? The answer is, not very. Its data would not be subject to verification. Since nationality is to be recorded "as declared" and so transmitted in downstream documentation, any number of non-citizens could instantly register themselves as Indian nationals. They could as easily open bank accounts, obtain Indian travel documents, and get jobs as genuine Indians. This obviously has negative security consequences. These should not be exaggerated. But the fact is that the UID is full of verification and authentication voids.

Even worse, the technology involved in it is highly problematic. A London School of Economics (LSE) team analysed a similar project considered by the British government. It concluded: "The technology envisioned... 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 problems will get immensely magnified in India, which is almost 20 times more populous than Britain and has a rickety administrative system.

The issue of the reliability of IT-based methods is ignored in India, thanks to blind faith in IT. This society is bewitched by technology but has a poor appreciation of science or the scepticism it counsels. Thus, we refuse even to countenance problems of data security and vulnerability to manipulation of electronic voting machines (EVMs), although these are widely recognised in technologically more literate societies - and although IT professionals based at the University of Michigan have successfully hacked into Indian EVMs ( The Times of India, May 21).

The UIDAI's database will be preyed upon by numerous agencies, Indian and foreign, commercial and governmental, security-related or involved in industrial espionage. Recently, researchers from the University of Toronto exposed a China-based computer espionage network that pilfered classified documents from India's Defence Ministry. The "compromised" installations included the Directorate-General of Military Intelligence; three Air Force bases; Indian Military Engineer Services in four places; a Mountain Artillery Brigade in Assam; two Indian military colleges; and Indian Embassy computers in Kabul, Moscow, Dubai, and Nigeria (see <http://nytimes.com/2010/04/06/science/06cyber.html>). Similarly, DNA databases can be corrupted, potentially victimising innocent citizens.

Nothing suggests that the UIDAI-related databases will be more secure than military networks. There is, besides all these weighty considerations, the question of costs of creating and maintaining an enormous database of 1.2 billion citizens. The LSE study estimated that the cost in Britain would be £10-20 billion. The proportionate cost in India would exceed Rs.2 lakh crore, enormous for a poor country, where 70 per cent of the population has no toilets. This means forgoing increased provision of public services.

In an interview to CNN-IBN, Nandan Nilekani does not deny that "this is a project where we are going into uncharted territories, the technological challenges are immense and one of the risks of the project is technology" (<http://www.hindu.com/thehindu/nic/nandannilekani.htm>). He also concedes that "I don't know what the exact figure... is", but still contends that "it is much less than [Rs.1.5 lakh crore]... by a factor of 10".

### **Violation of privacy**

However, all these grave problems pale beside the UID's potential for invading citizens' privacy and violating constitutional freedoms.

NATGRID will provide security agencies real time access into 21 categories of databases - including bank account details, credit card transactions, driving licences, and visa and immigration records. An intelligence official has been quoted as saying: "Once you feed in a person's name, you'll get all the details about him, across all databases." These include overdue traffic fines and credit card records. "There really will not be any secrets from the state."

The data collected would greatly exceed the need-based information that people furnish to different agencies to operate a bank account, obtain a passport or get a ration card. Now all this information will be pooled and made to converge in a single database available to hundreds of government departments at the click of a mouse.



**VIJAY KUMAR JOSHI/PTI**

*Nandan Nilekani, UIDAI chief:  
"The technological challenges are huge."*

This convergence means that the citizen will lose control over his/her personal information. Official agencies can use this information to track citizens' movements, bank transactions and other legitimate activities. This constitutes an impermissible intrusion by Big Brother into privacy, a fundamental right.

The NPR and NATGRID can track and profile individuals by studying transactions and patterns. The NPR is being compiled not under the Census Act but under the Citizenship Act, 1955. The



Census Act guarantees confidentiality and says personal data is "not open to inspection nor admissible in evidence". Such protection is missing from the latter, which makes citizen registration "compulsory". The Census Act aims at capturing the profile of the population, not individuals. Profiling of individuals is liable to violate their freedom, privacy and confidentiality.

However, strangely, the UIDAI disowns all responsibility for how its database will be used. It openly declares it is in "the identity business". It states: "The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies." Also, "the UID number will only guarantee identity, not rights, benefits or entitlements". This falsifies the key rationalisation offered for the scheme: namely, that the UID will break the barriers that prevent the poor from accessing public services/subsidies.

The Indian state's record of abusing technology and personal information is deplorable. Take the recent tapping of politicians' conversations by agencies using new "passive interception technology", which enables them to eavesdrop on all mobile communication within a 2-km radius. This led to an uproar in Parliament. But the government is planning to legalise the use of such equipment while short-circuiting the procedure for wiretapping under the Telegraph Act, which requires the approval of the Home Secretary and review by a high-level committee headed by the Cabinet Secretary.

The state has always tried to acquire extraordinary powers over citizens and then abuse them. One only has to recall the record of implementation of our preventive detention laws, TADA, POTA and the more than 200 other extraordinary laws such as the Public Security Acts of many States to be gravely concerned at the abuse potential. What India needs is not the UIDAI, but effective legisla-

tion to defend privacy and punish intrusion into it.

The intelligence agencies are not answerable to the public and are outside the purview of the Right to Information Act. We can never know what they know about citizens and how they interpret and use this information. The UID scheme and associated database-sharing will enable state agencies to know every minute detail of a citizen's life, but the citizen is barred from knowing what they know about him/her and what they do with that knowledge. This is a mockery of democracy.

This society is already paying heavily for the state's practice of the politics of suspicion, whose most extreme expression is "encounter killing". The National Human Rights Commission (NHRC) recently admitted that as many as 2,560 police "encounters" were reported to it between 1993 and 2006 - an annual average of 183. It found almost half - 1,224, to be precise - to be "fake" or staged, that is, non-judicial executions.

The state behaves particularly roguishly when acting in the name of defending national security. Experience tells us that the key to fighting terrorism is to treat it as a crime and bring its perpetrators to book while addressing its root causes. What is needed is not more intrusive surveillance, nor more sophisticated electronic databases, but good, honest policing, patient collection of evidence and competent prosecution.

To put yet more draconian and unaccountable powers in the hands of the state is to write the charter of citizens' slavery. The UID project does exactly that. It must be uncompromisingly opposed. Or else, we will slide down the slippery slope of strangling people's freedoms and rights and using increasingly intrusive means to "discipline" citizens. Nothing can harm democracy more grievously.

# (N)PR, A FRAUD, ANTI-NATIONAL VENTURE

---

S GURUMURTHY

---

'The population enumeration in the Census 2011 has nothing to do with the citizenship issues under the citizenship law at this stage, because the census does not involve any preparation of 'National Population Register' (NPR) now, but only the collection of information for the preparation of NPR later.' This is what the Union home minister means in his statement on the Census 2011 in Parliament (May 7). The acute legalism in the minister's statement conceals the truth and presents a fake view of the population census for the NPR, thus totally whitewashing this ongoing fraud on the nation.

Start with what is undeniably a lie, even forgery. The title 'National Population Register' is itself faked. Neither the Indian Citizenship Act 1955 nor the Citizenship Rules 2003 speak of any 'National' Population Register. The Citizenship rules talk about just 'Population Register'. The omission of the prefix 'National' here is no accident. It is intentional. This is self-evident from the citizenship rules, which, in the same breath, talk of 'National Register of Indian Citizens' (NRIC). The use of the prefix 'National'

there is intentional in contrast. The reason why the Population Register is not similarly prefixed with 'National' as in the NRIC is obvious. The lawmakers knew that the Population Register is not a record of the Indian 'National' Population. That is why the Citizenship law titles it as 'Population Register', that is, it is 'PR', not '(N)PR'. But how then did the prefix 'National' get forged into the PR to make it (N)PR in the minister's statement? Will he explain?

Saying that 'the population census is the total process of collecting demographic, economic and social data' the minister adds, 'the particulars in respect of the individuals are kept confidential'. He further says that 'the particulars collected' 'shall be verified' afterwards under the citizenship law, and cases of 'doubtful citizenship' will be dealt with appropriately. Thus, the minister implies -- yet not says explicitly -- that the ongoing population census is not under the citizenship law, but exclusively under the census law. But, as the analysis here unfolds, the minister's explanation that what the Census 2011 does is just to collect data for the Population Register and that the verification of the information would take place under the citizenship law later, is patently untrue, why, even a lie. A seer is needed to discover this? No.

The website of the minister's own home department on Census 2011 uncovers it. The census manual in the website says: "the field-work of the House-listing and Housing Census and the National Population Register are being conducted simultaneously by the same enumerator". And the answer to one of the FAQs in the website

<http://censusindia.gov.in/2011-FAQ/FAQ-Public.html> says: "The Census is a statutory exercise conducted under the provisions of the Census Act 1948 and Rules made there under. The NPR is being created under the provisions of the Citizenship Act and

Rules." So, admittedly, Census 2011 creates the PR under the citizenship law. And it involves enumeration under both laws -- for housing under the census law and for population under the citizenship law. Does the minister's statement that the census is purely a data collection under the census law just now survive the truth in his own website?

Now test the Union home minister's statement on the rules under the citizenship law. The data for Population Register (PR) and National Register of Indian Citizens (NRIC) are collected under the citizenship law and rules, not the census law. The citizenship rules provide for population census thus: the government shall conduct house-to-house enumeration to collect details 'including the citizenship status'; and the Registrar General of Citizen Registration (RGCR) under the citizenship law shall notify the period and duration of the enumeration. The particulars to be collected for the PR are also mentioned in the citizenship rules. So, the enumeration for PR is prescribed under the citizenship law, not census law. Therefore, the minister's claim that the enumeration is under the census law and the later verification will be under the citizenship law is patently untrue.

The implication in his statement that the name of the registrar general, who is the authority under the census as well as citizenship laws, may have led to misunderstanding in the sense that he is involved from the side of the citizenship law, is deceptive. This subterfuge conceals the fact that the population details now being gathered are actually under and as prescribed in -- but without complying with -- the citizenship rules. But for this subterfuge, the minister will have to concede that the query in the ongoing enumeration, the Query No 11, to the effect 'citizenship as declared' is not only contrary to the citizenship law, but is actually a fraud on the law. Read on, with some patience as it is all about law.

It is the citizenship rules, not the census law, that provide for both the collection and verification of the population data. It is not that, as the minister pretends, information is collected under the census law now and verification takes place, later, under the citizenship law. Just take one mandate in citizenship rules. The citizenship rules direct that 'during the verification process, particulars of such individuals whose citizenship is doubtful shall be entered with appropriate remark in the Population Register.'

Unless the enumerators are first asked to notice cases of doubtful citizenship, how will such cases come up for verification at all?

But, instead of asking them to notice and record the cases of doubtful citizenship during enumeration, see how the census manual directs the enumerators to fill the space against Query No 11 'Nationality for each of the enumerated person has to be asked from the respondent and recorded. .... Please record the nationality of the respondent as declared by her/him for each of the persons enumerated. Do not get into any argument with the respondent regarding this.'(See Para 5.21.1 of general instructions). That is, when the citizenship rules ask for doubtful cases of citizenship to be identified, the census manual to collect details under the very citizenship rules virtually says 'don't doubt the respondents on their claim of nationality; just record what they say.' How then will suspect cases of citizenship be discovered? Clearly, the ongoing enumeration is not intended to discover suspect citizenship, but to suppress them, and make them appear genuine. Can the minister deny that Query No 11, read with the census manual, exposes his lie?

Shockingly, anyone who had entered into India six months before the census, or any one who intends to stay for six months after, becomes a 'usual resident' under the ongoing census rules. Such persons, thanks to the census, can declare themselves as

Indian citizens in response to Query No 11. And more shockingly, the government proposes to issue 'National Identity Cards' to all such people even though under the law, 'National Identity Cards' are allowed only for Indian citizens.

Imagine, like Kasab who did the mayhem in Mumbai on 26/11, a Pakistani enters India today and promises to be here for six more months, he is eligible to declare himself as an Indian citizen in response to Query No 11, also get a National Identity Card. He will be an Indian terrorist, not a Pakistani jihadi. According to intelligence sources, some 40,000 Pakistanis have entered India and after throwing their passports away, they have melted into Muslim- dominated areas. Under the Census 2011 they are 'usual residents', can declare themselves as Indian citizens and will now get National Identity Cards. After all the enumerators are directed to not to argue with them when they declare their nationality as Indian, and to just write as they claim.

**QED: The ongoing population census is undoubtedly an anti-national venture. It is placing millions of timeless bombs all over India. Is the home minister, who seems lost in legalisms, aware?**

*(The writer is a well-known commentator on political and economic issues. E-mail: comm...@gurumurthy.net)*

## COPYRIGHT AND PRIVACY

INDIA'S copyright act was established in 1857; it has most recently been amended in 2010. Even though India currently is not a member of WIPO, the provisions in the proposed Bill will work to make the act WIPO compliant. When looking at privacy in the context of copyright four key questions arise:

### **How do DRM technologies undermine privacy and what safeguards are present in the Indian Law to protect citizens right to privacy?**

Technologies such as digital rights management technologies were developed to be used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. DRM technologies pose as a privacy threat, because in their ability to monitor what is happening to a copyrighted work, they are also able to collect personal information and send it back to a host without knowledge of the user. The host is then able to use that data for marketing or commercial purposes. In the Copyright Act 1957 there are no current provisions against DRM circumvention. In the proposed Copyright Bill 2010 there are two proposed provisions, to prevent anti circumvention of DMR technologies, and one provision that clarifies what is a DMR technology.

### **Proposed Legislation**

**Section 2 (xa):** Defines Rights Management information.



**Section 65A :** Protection of Technological Measures - Any person who knowingly makes or has in his possession any plate for the purpose of making infringing copies of any work in which copyright subsists shall be punishable with imprisonment which may extend to two years. The section includes that any person facilitating circumvention by another person of a technological measure, shall maintain a complete record of such other persons including his name, address and all relevant particulars necessary to identify him.

**Section 65B:** Protection of Rights Management Information - Any person who removes or , distributes, copies or broadcasts any rights management information without authority shall be by punishable with imprisonment.

**Recommendation:** We find that in this provision the privacy of an individual is brought into question, because there are no safeguards against the commercialization of information, and no formal process of redress if an individual discovers that his information is being used without his consent/prior knowledge. We would recommend that it be clearly articulated in the provision that the collection and commercialization of information and personal data is prohibited by DRM technologies and host companies, and a method of redress be put in place.

**Under the copyright does a person have the ability to expose privacy infringement?**

Because DRM technologies often employ the use of spy-ware, it is important that an individual has the ability to know if spy-ware is being used on their computer systems. Currently reverse engineering is permitted under provision 52 (ac). The amended version of provision 52 is less clear on if reverse engineering would be allowed.

**Current Legislation:**

**Provision 52 (ac):** Certain acts not to be in infringement of copyright include..the observation, study or test of functioning of the computer programs in order to determine the ideas and principles which underlie any elements of the program while performing such acts necessary for the functions for which the computer program was supplied The following acts shall not constitute in infringement of copyright, namely:

**Proposed**

The proposed amendment reads:

- 52 (1) The following acts shall not constitute n infringement of copyrights, namely:
- (i) (a) a fair dealing with a literary, dramatic, musical or artistic work not being a computer program for the purposes of:
  - (ii) private use, including research
  - (iii) Criticism or review, whether of that work or of any other work.

The exclusion of computer program in the proposed bill, makes it unclear under what circumstances reverse engineering would be allowed.

**Recommendation:** We would recommend that for clarity purposes a specific clause be added to the act that details under what circumstances a person is allowed to reverse engineer a product for protection of their own privacy.

### **3. How does the proposed exception for the disabled undermine privacy?**

In India the current Copyright Act 1957 there are no provision for the benefit of disabled persons, thus currently permission from copyright holders needs to be exclusively sought every time the visually challenged person requires access. Under the Constitution of India and the Berne Convention India has committed to enshrining the rights of the disabled.

#### **Proposed Legislation**

The proposed amendment of the act will grant compulsory license in respect of publication of any copyrighted works not covered by the exception under section 52 (1) (zb)

The Bill also proposes a board that would establish the credentials of the applicant and satisfy itself that the application has been made in good faith. This compromises the anonymity that most individuals enjoy when a disabled person tries to access a digital library.

**Recommendation:** We recommend that the proposed Bill limits the authentication process a disabled person must go through when accessing digital libraries etc, and the extent to which records are to be kept of transaction This will serve to protect the anonymity and privacy of disabled persons..

### **4. What is On the Horizon?:**

As copyright and IP is a constantly evolving issue, countries are consistently amending and changing their laws. With the flow of peoples across borders increasing, Indians will be affected by different international policies that could pose to infringe upon their privacy, for example cross border checks or three strike regimes.

**Examples of Proposed Legislation:** The Anti- Counterfeiting Trade Agreement:

ACTA is a proposed legislation with the objective to combat counterfeiting and piracy. Partners in the negotiations include: The United States, Australia, Canada, the European Union, Japan, Mexico, Morocco, New Zealand, Singapore, South Korea, and Switzerland. The treaty will oblige each Contracting Party to adopt, in accordance with its legal system, the measures necessary to ensure the application of the treaty. Though ACTA has not been enacted, many worry that ACTA would facilitate privacy violations by trademark and copyright holders against private citizens suspected of infringement activities without any sort of legal due process. The act would could allow for random searches of laptops, MP3 players, and cellular phones for illegally downloaded or ripped music and movies.

**Recommendation:** We find that copyright infringement does not appear to justify a three strike regime or cross border searches. ACTA and other international treaties raise the question that if India became compliant with certain international standards, the standards would be too stringent without safeguards, and pose as a risk to a persons privacy.