



AN APPEAL TO PARLIAMENTARIANS - Reasons why you should oppose the UID Bill

The draft National Identification Authority of India (NIDAI) Bill will be placed before the Lok Sabha in the current session. Touted by its promoters as a landmark initiative for “good governance”, the concept and basic premise of the Bill has been critiqued and challenged on multiple grounds by experts as well as ordinary citizens.

Here are some reasons why you should oppose and vote against the bill when it is placed before the House.

1. False claims

The Government of India and Nandan Nilekani, Chairperson UIDAI, have been claiming that the UID scheme will enable inclusive growth by providing each citizen with a verifiable identity, that it will facilitate delivery of basic services, that it will plug leakages in public expenditure and that it will speed up achievement of targets in social sector schemes.

These claims are false and unjustified. Exclusion and leakages are not caused by the inability to prove identity – they are caused by the deliberate manipulation of the system by those who have the power to control the flow of benefits.

For instance, BPL families who have valid ration cards are unable to get their quota of foodgrains – not because the validity of the card is disputed, but because the ration shop owners exploit them and force them to take less than their due.

Scholarships meant for them are denied to children from Dalit families – not because they cannot prove they are Dalits but because teachers and school administrators pocket the money after forcing the parents to sign on false receipts.

Women workers in NREGA are paid less than their due – not because they cannot prove that they have put in the full quota of work, but because the supervisors and paymasters believe that women do not deserve the same wage as men, and pocket the extra money.

None of these problems will be solved by the possession of a UID number. In fact, a confidential working paper prepared by the UIDAI states that “the UIDAI is only in the identity business. The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies – the job of tracking distribution of food grains among BPL families for example, will remain with the state PDS department. The adoption of the UID will only ensure that the uniqueness and singularity of each resident is established and authenticated, thereby promoting equitable access to social services.”

In other words, the possession of a UID card can at best serve only as proof of a “unique and singular” identity and does not guarantee either citizenship or benefits. This being the case, it is strange that this scheme is touted as a step for good governance.

2. Violation of privacy and civil liberties

The UID scheme violates the right to privacy. International law and India’s domestic law have set clear standards to protect an individual’s privacy from unlawful invasion. Under the International Covenant on Civil and Political Rights (ICCPR), ratified by India, an individual’s right to privacy is protected from arbitrary or unlawful interference by the state. The Supreme Court has also held the right to privacy to be implicit under article 21 of the Indian Constitution (Rajagopal v. State of Tamil Nadu, 1994 and PUCL v. Union of India, 1996). India has enacted a number of laws that provide some protection for privacy. For example the Hindu Marriage Act, the Copyright Act, Juvenile Justice (Care and Protection of Children) Act, 2000, the Indian Contract Act

and the Code of Criminal Procedure all place restrictions on the release of personal information.

Section 33 of the draft bill empowers NIDAI to disclose personal data on an order of a court or in case of “national security” on directions of an officer not below the rank of joint secretary. This is a dilution of existing provisions for protection of privacy under Supreme Court judgments (PUCL versus Union of India) and the IT and Telegraph Acts, all three of which state that such orders can be passed only by the Union or State Home Secretary. There is a high likelihood of this provision being misused by persons in power to access private details for use in ways that may pose a risk to the life or security of the person concerned.

Personal and household data is being collected through the Census 2010 with a view to establishing a National Population Register. It is proposed to make this information available to the UIDAI. This is in contravention of Section 15 of the Census Act which categorically states that information given for the Census is “not open to inspection nor admissible in evidence”.

Moreover, although participation in the UID scheme is supposed to be voluntary and optional, Census respondents are being told that it is mandatory to submit personal information for the National Population Register. The enumerators who are collecting data for the Population Register have been instructed to flag the details of “doubtful cases” who will then be subject to further investigation to determine whether they are “genuine citizens”. Enumerators are generally not able to explain the criteria for categorising a particular individual or family as “doubtful”.

3. “Functionality creep” and misuse of data

The centralised database where personal data will be stored can easily be linked with other databases, such as the Employees' State Insurance Corporation and databases maintained by the police and intelligence agencies. This raises the risk of “functionality creep”, as for instance the use of the UID database for policing and surveillance.

There is a serious concern that the biometric information collected as part of the UID project would be used for policing purposes. The regular use of biometric data in policing can lead to a large number of human rights violations, especially given the possibility of errors in fingerprint matching.

The proposed Bill does not contain any mechanisms for credible and independent oversight of the UIDAI. This increases the risk of ‘functionality creep’ - the government may add features and additional data to the database without informing or taking the consent of citizens and without re-evaluating the effects on privacy in each instance.

There is no guarantee that the personal data collected and stored in a centralised database will not be misused for purposes other than mere confirmation of identity. The several instances of the involvement of the state in mass carnage (as in Delhi in 1984 and Gujarat in 2002), and the Government's support to and defence of the widespread use of “encounter killings” and other extra-constitutional methods by the police and armed forces, has already created an enabling environment for abuse of the UID database to serve undemocratic, illegal and unethical purposes.

The Bill does not have any provisions to penalise misuse of data by authorised persons (eg UIDAI officials), and therefore has an in-built potential for use of personal data to identify and eliminate “maoists”, “terrorists”, “habitual offenders”, political opponents and others who are perceived as threats by those in power.

4. Inappropriate and unproven technology

Instead of facilitating inclusion, around 150 million people are likely to be excluded from benefits because of the UID scheme.

Millions of Indians working in agriculture, construction workers and other manual labourers have worn-out fingers due to a lifetime of hard labour, resulting in what is technically referred to as ‘low-quality’ fingerprints. These are precisely the people who are currently excluded from government records and welfare schemes.

This means an NREGA beneficiary with worn-out fingers may present his newly-issued UID number as a conclusive proof of identity to claim payment, but could find the application rejected. The authentication

process using a fingerprint scanner could classify the applicant's worn-out fingers as a so-called 'false negative'. This is a serious concern, since NREGS has been listed as one of the pilot schemes where the UID identification process will be introduced - the 30 million people currently holding NREGS job cards will be put at risk of exclusion.

This limitation is well recognised by the UIDAI in its working paper, which states that fingerprint authentication is not foolproof, since multiple factors (such as the degree and direction of the pressure applied while placing the finger on the sensor, excessively greasy or dry skin, and distortions caused by rendering a three-dimensional object into a flat plane) can result in "noise and inconsistencies" in the captured image. According to the paper, these distortions result in impairing the system performance and consequently limiting the widespread use of this technology".

The other biometric data to be collected by the UID are iris scans and photographs. An iris scan cannot be done on people with corneal blindness, glaucoma or corneal scars. There are an estimated 6-8 million people in India with corneal blindness, according to researchers at the All India Institute of Medical Sciences, New Delhi. The number of people with corneal scars (caused by infections or injuries to the eyes) will be much more. It is reported that Cabinet Secretary K.M.Chandrasekhar has opposed the collection of iris scans, terming it a "waste of money."

5. Database security not assured

India does not have a robust legal framework or infrastructure for cybersecurity and has weak capabilities in this area – several of our high-security databases have been hacked in the recent past. The huge amounts of personal information collected in the UID database will most likely not be adequately protected and will be vulnerable to hackers and identity thieves.

It is important to note that no country or organisation has successfully deployed a database (biometric or otherwise) of the size envisioned for the UID project, and no technical or corporate body in the world has the experience necessary to ensure its security.

The possibility of corruption and exploitation of data is far greater in a centralised database than when the information is dispersed across different databases. There is also a high risk of errors in the collection of information, recording of inaccurate data, corruption of data and unauthorised access.

Other countries with national identification systems have tried and failed to eliminate the risks of trading and selling of information. India, which has no generally established data protection laws (like the U.S. Federal Privacy Statute or the European Directive on Data Protection) is ill-equipped to deal with such problems.

The US - arguably the most surveillance-prone society in the world - passed a Federal law (the REAL ID Act, 2005) requiring the States to allow the Federal Department of Homeland Security to access State databases such as drivers' licences and motor vehicle registration. As of 2008, not a single State has ratified this Act, and 25 States have passed legislations to exclude themselves from its purview.

Ironically, a confidential working paper titled "Creating a Unique Identity Number for Every Resident in India" was recently posted on the transparency website Wikileaks. The leaked document admits that "the UID database will be susceptible to attacks and leaks at various levels".

If they cannot protect their own confidential documents, we cannot trust the UIDAI to protect the data they propose to collect from us.

6. Unjustifiable costs

The UID project has been launched without a feasibility study or cost-benefit analysis. The current costs are estimated at Rs.45,000 crores. A budget provision of Rs. 1950/- Crores has been made for the current year, of which over 200 crores has already been spent.

Nandan Nilekani claims that several thousand crores of rupees would be saved by the scheme, through prevention of duplicate/fake IDs for claiming benefits under schemes such as the public distribution system and the NREGS. This claim has not been supported with data, and is not substantiated by any studies so far.

Operationalising the UID scheme on the ground for NREGA and the public distribution system would require placing fingerprint readers at every *panchayat* office and every ration shop. The cost of a fingerprint reader at this time is around USD 50. The total costs of placing fingerprint readers in each PDS outlet and in each of India's 600,000 villages have not been taken into account in official cost calculations.

Verification of identity by the UIDAI will be charged at Rs.10 per query. This being the case, several private agencies may bypass the UIDAI and give preference to other identity proofs.

7. Bypassing of Parliament and democratic processes

The UID Authority has been set up with considerable powers and resources, without any approval from Parliament or discussion in the public domain about the necessity of such a scheme. In the absence of a Constitutional provision or legal framework (such as that set out in the proposed Bill), all the actions of the UIDAI are technically unconstitutional and illegal. There is no transparency either on decisions or on expenditure, no oversight and no mechanisms for accountability in the functioning of the UIDAI.

Nandan Nilekani has been given sweeping powers, and is now demanding the right to select "good officers" to serve under him, bypassing the usual procedures for deputation of officers.

Despite the continuing debate on public platforms, and being repeatedly questioned about the risks, costs and benefits of the UID scheme, Nilekani and the Government of India have remained silent on the contested aspects of the scheme.

8 Lessons from other countries

Several countries (including the USA, the UK, Australia, China, Canada and Germany) have tried such projects and have given these up as impractical, unjustified and dangerous.

One of the first acts of the new government in UK after taking office in June 2010, was to scrap the UID project in that country. According to Theresa May, the UK Home Secretary, "The national identity card scheme represents the worst of government. It is intrusive and bullying. It is ineffective and expensive. It is an assault on individual liberty that does not promise a great good...The government will destroy all information held on the national identity register, effectively dismantling it. The role of the identity commissioner, created in an effort to prevent data blunders and leaks, will be terminated."

It is noteworthy that the reasons cited by the UK government for rejection of the UID scheme - higher costs, impracticality and ungovernable breaches of privacy and civil liberties – are all valid in the Indian case as well. In view of this, it is fair to expect UIDAI to present a comprehensive argument to justify why what was rejected in the UK is good enough for India.

It seems clear that the public pronouncements on the UID scheme being a step towards good governance and inclusive growth are red herrings to divert the attention of the public from the real purpose of NIDAI – to strengthen India's e-surveillance capabilities!

The passage of the IT Act, 2008, was the first step to making India a country where "Big Brother" is watching everyone, all the time – the NIDAI Act will be another great leap forward in this direction!

**Please do not remain silent -
oppose the NIDAI Act
to defend democracy & protect human rights.**

**CONTACT: A CAMPAIGN FOR NO UID, C/o. INDIAN SOCIAL ACTION FORUM (INSAF),
A124/6 1st floor, Katwaria Sarai, New Delhi 110 016.**

Tel: +91-11-26517814/ 65663958; Fax: 011-26517814; Email: insafdelhi@gmail.com

Alternative Law Forum, Citizen Action Forum, Delhi Forum, PEACE, People's Union for Civil Liberties (PUCL) – Karnataka, Moving Republic, Indian Social Action Forum (INSAF), National Campaign for Dalit Human Rights (NCDHR), Slum Janandolana – Karnataka, The Center for Internet and Society (CIS) **and many other organisations and concerned individuals.**

