Infopack

JANUARY, 2011

Popular Information Centre

EDITORIAL

UID: Facilitating Delivery or Targeting Citizenry?

- Piyush Pant

If Government of India's intention is given a go, then soon the whole of India will become a prison house and all Indians prisoners who will be identified not by their names etc. but by Unique Numbers (Qaidi No….) allotted to them by a cabinet appointed authority named UIDAI (Unique Identification Authority of India). Being done in the name of better and efficient delivery of Government services to the poor by plugging leakages, the whole exercise appears unconstitutional, illegitimate, anti-people, restrictive of civil liberties and violating the privacy of the citizens. The purpose of this exercise is said to build the National Population Register.

The National Identification Authority of India Bill (NIAI), 2010 was introduced in Rajya Sabha in early December 2010, nearly two years after Unique Identification Authority of India (UIDAI) was established in February 2009 not through parliamentary exercise but merely by a cabinet decision, Prime Minister Manmohan Singh himself handpicking Nandan Nilekani its chairman. The NIAI Bill is primarily aimed at making the UIDAI a legally sanctioned body and setting out its powers and functions.

UIDAI has been created to give each Indian resident a UID or Aadhaar number. This will be a unique 12-digit number which will store basic demographic and identity information of an individual along with his/her biometrics (10 fingerprints, iris scan and photo). It is being said that this will be a dream cum true for the intelligence agencies for they will be having everyone's fingerprints at the click of a mouse, that too with demographic information and all the rest. That's why doubts are being raised regarding the real intent of the bill. It is being pointed out that the real motive behind setting up the Authority is the surveillance of the citizens in order to pick and choose the ones who have guts to criticize the State policies and to stand and speak out in support of marginalized people.

This is to be remembered that the UID project owns its origin to the controversial report of the Kargil Review Committee which said that urgent steps were needed to issue ID cards to the villagers in border districts, pending its extension to other parts of the country. During the NDA regime, a report by a Group of Ministers had conveyed that all citizens must be given a multi purpose national identity card (MNIC) and non-citizens should be issued identity cards of a different colour and design so as to check illegal migration. The Citizenship Act of 1955 was amended in 2003, soon after the MNIC was instituted. This way the privacy clauses in Census surveys were significantly diluted in 2003 itself. When UPA government first came into power in 2004, it took forward the plans of the NDA government under a new name. The MNIC project got replaced by UID project in January 2009 in which security concerns were replaced by developmental concerns. Thus it appears that NDA, through this project, wanted to prevent the Bangladeshi migrants from becoming substantial vote-bank for their rival parties while UPA II seems intending to target the saner voices in the name of 'War against Terrorism' and fighting Maoism.

Another vital concern being raised against the bill is that it will take away the privacy of individuals. It is being pointed out that the concerns of privacy or civil liberties are not discussed in any of the documents of the government.

In this issue of **INFOPACK**, summary of such documents is given which elaborate on various aspects of the controversial **UID project in India**.

The National Identification Authority of India Bill, 2010

Proposed Draft Bill

By:

By Government of India

Bird's Eye View

The document points out that this Bill will be enacted in the Parliament in the Sixty-first Year of the Republic of India. The objective of the Bill is to provide for the establishment of the National Identification Authority of India for the purpose of issuing identification numbers to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access to benefits and services to such individuals to which they are entitled.

The 19-page document in divided into eight chapters:-

Chapter I: Preliminary (Short title, extent, commencement and definition;

Chapter II: Aadhar Numbers;
Chapter III: National Identification Authority of India;
Chapter IV: Grants, Fund, Accounts and Audit and Annual Report;
Chapter V: Identity Review Committee;
Chapter VI: Protection of Information;
Chapter VII: Miscellaneous.

In **Chapter I**, the document says that this Act may be called the National Identification Authority of India Act, 2010, and shall extend to the whole of India except the State of Jammu and Kashmir. The Act will come into effect on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act.

In this chapter, the document also gives a list of some important definitions related to this Act. For example,

a) "aadhar number" means an identification number issued to an individual under sub-section (2) of the section 3;
b) "aadhar number holder" means an individual who has been issued an aadhar number under this Act;
c) "Authority" means the National Identification Authority of India established under sub-section (1) of section 11;
d) "authentication" means the process wherein aadhar number, along with other attributes (including biometrics) are submitted to the Central Identities DATA Repository for its verification and such Repository verifies the correctness thereof on the basis of information or data or documents available with it.
e) "biometric information" means a set of such biological attributes of an individual as may be specified by regulations;
f) " Central Identities Data Repository" means a centralized database in one or more locations containing all aadhar numbers issued to aadhar number holders along with the corresponding demographic and biometric information of such individuals and other information related thereto;
g) "demographic information" includes such information relating to the name, age, gender and address of an individual (other than race, religion, caste, tribe, ethnicity, language, income or health), as may be specified in the regulations for the purpose of issuing an aadhar number;
h) "Identity information" in respect of an individual means biometric information, demographic information and aadhar number of such individuals.

In **Chapter II**, the document talks about **Aadhar Numbers and properties and authentication of aadhar numbers**. It says that every resident shall be entitled to obtain an aadhar number on providing his demographic information and biographic information to the Authority in such manner as may be specified by regulations:

Provided that the Central Government may, from time to time notify such other category of individuals who may be entitled to obtain an aadhar number.

The aadhar number, issued to an individual shall not be reassigned to any other individual.

The aadhar number shall be a random number and bear no attributes or identity data or part thereof, relating to the aadhar number holder.

The aadhar number shall, subject to authentication, be accepted as proof of identity of the aadhar number holder.

The document also says that the Authority shall perform authentication of the aadhar number of an aadhar number holder in relation to his biometric information and demographic information subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.

The aadhar number or the authentication thereof shall not, by itself, confer any right of or be proof of citizenship or domicile in respect of an aadhar number holder.

The Authority may require the aadhar number holders to update their demographic information and biometric information, from time to time, in such a manner as may be specified by regulations so as to ensure continued accuracy of their information in the Central Identities Data Repository.

The Authority shall take special measures to issue aadhar number to women, children, senior citizens, persons with disability, migrant unskilled and unorganized workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations. Identification Authority of India. It says that the

In **Chapter III**, the document talks about **National Identification Authority of India**. It says that the Central Government shall, by notification, establish an Authority to be known as the National Identification Authority of India to exercise the powers conferred on it and to perform the functions assigned to it under this Act.

The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provision of the Act, to acquire, hold and dispose of property, both movable and unmovable, and to contract, and shall, by the said name, sue or be sued.

The Authority shall consist of a Chairperson and two part time Members to be appointed by the Central Government.

The Chairperson shall not hold any other office during the period of holding his office in the Authority as such.

The Central Government may remove from office the Chairperson, or a Member, who -

a) is, or at any time has been adjudged as insolvent;
b) has become physically or mentally incapable of acting as the Chairperson or, as the case may be, a Member;
c) has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude;
d) has acquired such financial and other interest as is likely to affect prejudicially his functions as the Chairperson or, as the case may be, a

Member, or

e) has, in the opinion of Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

The document further says that the Chairperson or the Member shall not be removed under clause (d) or clause (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard in the matter.

The Chairperson or a Member, ceasing to hold office as such, shall not, without previous approval of the Central Government, accept any employment in, or connected with the management or administration of, any person which has been associated with any work under the Act, for a period of three years from the date on which they cease to hold office.

The Chairperson shall have powers of general superintendence, direction in the conduct of the affairs of the Authority (including all its decisions) and he shall, in addition to presiding over the meeting of the Authority, and without prejudice to any of the provisions of this Act, exercise and discharge such powers and functions of the Authority as may be prescribed.

There shall be a chief executive officer of the Authority, not below the rank of the Additional Secretary to the Government of India, who shall be the Member-Secretary of the Authority, to be appointed by the Central Government. The chief executive officer shall be the legal representative of the Authority and shall have administrative control over the officers and other employees of the Authority.

The document also says that on and from the establishment of the Authority, all the assets and liabilities of the Unique Identification Authority of India, established vide notification of the Government of India in the Planning Commission number A-43011/02/2009- Admin.I, dated the 28th January, 2009, shall stand transferred to, and vested in, the Authority.

The Authority shall develop the policy, procedure and systems for issuing aadhar numbers to residents and perform authentication thereof under this Act.

Without prejudice to the provisions contained in sub-section (1), the powers and functions of the Authority may, inter alia, include all or any of the following matters, namely:-

- establishing, operating and maintaining of the Central Identities Data Repository;
- sharing, in such manner as may be specified by regulations, the information of aadhar number holders, with their written consent, with such agencies engaged in delivery of public benefits and public services as the Authority may by order direct;
- specifying by regulation, various processes relating to data management, security protocols and other technology safeguards under this Act;
- specifying by regulation, the conditions and procedures for issuance of new aadhar number to existing aadhar number holder;
- levy and collect the fees or authorize the Registrars, enrolling agencies or other services providers to collect such fees for the services provided by them under this Act in such manner as nay be specified by regulations.

In **Chapter IV**, the document talks about **Grants, Fund, Accounts and Audit and Annual Report**.

It says that the Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority, grants of such sums of money as the Central Government may think fit for being utilized for the purposes of this Act.

The fund may be applied for meeting -

1) the salaries, allowances and other remuneration of the Chairperson, Members and other officers and employees of the Authority; and
2) the other expenses of the Authority in connection with the discharge of its functions and for the purposes of this Act.

The Authority shall furnish to the Central Government at such time and in such manner as may be prescribed or as the Central Government may direct, such returns and statements and particulars in regard to any matter under the jurisdiction of the Authority, as the Central Government may from time to time require.

In **Chapter V**, the document refers to **Identity Review Committee**. It says that the Central Government may, by notification, constitute the Identity Review Committee consisting of three members to discharge functions specified under sub-section (1) of the section 29 in respect of any matter connected with the usage of the aadhar numbers.

The members of the Review Committee shall hold office for a term of three years from the date on which they enter upon office and shall not be eligible for re-appointment.

The Central Government may by order remove from office any member of the Review Committee, who-

(a) is, or at any time has been adjudged as insolvent;

(b) has become physically or mentally incapable of acting as a member;

(c) has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude;

(d) has acquired such financial or other interest as is likely to affect prejudicially his functions as a member; or

(e) has, in the opinion of the Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

The Review Committee shall ascertain the extent and pattern of usage of the aadhar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhar numbers along with its recommendations thereon and submit the same to the Central Government.

The copy of the report along with the recommendations of the Review Committee shall be laid by the Central Government as soon as may be after it is received, before each House of Parliament.

In **Chapter IV**, the document deals with **Protection of Information**. It says that the Authority shall take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

Save as otherwise provided in this Act, the Authority or any of its officer or other employee or any agency who maintains the Central Identities Data Repository (CIDR) shall not, whether during his service as such or thereafter, reveal any information stored in the CIDR, to any person.

In case any demographic information and any biometric information of a aadhar number holder is lost or changes subsequently, the aadhar number holder shall request the Authority to make necessary alteration in his record in the CIDR in such manner as may be specified by regulations.

On receipt of any request under sub-section (1) or sub-section (2), the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such aadhar number holder and intimate such alteration to the concerned aadhar number holder.

Every aadhar number holder shall be entitled to obtain details of request for authentication of his/her aadhaar number and the response provided thereon by the Authority in such manner as may be specified by regulations.

The same chapter also talks about **Offences and Penalties**. It says that whoever, with the intention of causing harm or mischief to an aadhar number holder, or with the intention of appropriating the identity of an aadhar number holder, changes or attempts to change any demographic information or biometric information of an aadhar number holder by impersonating or attempting to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information shall be punishable with imprisonment for a term which may extend to three years and with a fine which may extend to ten thousand rupees or with both.

The document also says that whoever, not being authorized to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorized to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorized under this Act shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Whoever, not being authorized by the Authority, uses or tampers with the data in the CIDR or any removable storage medium with the intent of modifying information relating to aadhar number holder or discovering any information thereof shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which may extend to ten thousand rupees.

Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Besides this, where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to, any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

For the purpose of sub-section (1), the provisions of this Act shall apply to any offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves the CIDR.

No penalty imposed under this Act shall prevent the imposition of any other penalty or punishment under any other law for the time being in force.

No court shall take cognizance of any offence punishable under this act, save on a complaint made by the Authority or any officer or person authorized by it.

In **Chapter VII**, the document refers to **Miscellaneous Provisions**. It says that notwithstanding anything contained in-

a) the Wealth Tax Act, 1957;

b) the Income-tax Act, 1961, or

c) any other law for the time being in force relating to tax, including tax on wealth, profits or gains or the provision of services.

The Authority shall not be liable to pay wealth-tax, income-tax or any other tax in respect of its wealth, income, profits or gains derived.

The document further says that if, any time, the Central Government is of the opinion,--

a) that, on account of circumstances beyond the control of the Authority, it is unable to discharge the functions or perform the duties imposed on it by or under the provisions of this Act; or

b) that the Authority has persistently defaulted in complying with any direction given by the Central government under this Act or in the discharge of the functions or performance of the duties imposed on it by or under the provisions of this Act and as a result of such default the financial position of the Authority or the administration of the Authority has suffered; or

c) that circumstances exist which render it necessary in the public interest so to do, the Central Government may, by notification, supersede the Authority for such period, not exceeding six months, as may be specified in the notification and appoint a person or persons as the President may direct to exercise powers and discharge functions under this Act.

Provided that before issuing any such notification, the Central Government shall give a reasonable opportunity to the Authority to make representations against the proposed supersession and shall consider the representations, if any, of the Authority.

The document also says that the Chairperson, Members, officers and other employees of the Authority shall be deemed, while acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act be bound by such directions on questions of policy, other than those relating to technical and administrative matters, as the Central Government may give, in writing to it, from time to time.

No suit, prosecution or other legal proceeding shall lie against the Central Government or the Authority or the Chairperson or any Member or any officer, or other employees of the Authority for anything which is in good faith done or intended to be done under this Act or the rule or regulation made thereunder.

The Central Government may, by notification, make rules to carry out the provisions of this Act.

The provisions of this Act shall be in addition to, and not in derogation of any other law for the time being in force.

If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty.

Anything done or any action taken by the Central Government under the Resolution of the Government of India, Planning Commission bearing notification number A-43011/02/2009-Admin.I, dated the 28th January, 2009, shall be deemed to have been done or taken under the corresponding provisions of this Act.

Creating a Unique Identity Number for Every Resident in India

By:

Unique Identification Authority of India

Wikileaks Document Release

13 November 2009

Bird's Eyeview

This forty-page document deals with Unique Identification Authority of India's (UIDAI) project on creating a unique identity number for every resident of India. This document is divided into eight chapters: 1) Executive Summery, Introduction, 2) The UIDAI Approach, 3) Enrolment into the UID, 4) Ensuring strong authentication, and what it means for the UIDIA, 5) Technology architecture of the UIDAI, 6) Legal framework, 7) Data security and fraud, 8) project execution and Project risk.

Under Executive Summery, the document says that in India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Every time an individual tries to access a benefit or service, the person must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand leading to increase in overall costs of identification and causing extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack documentations, and find it difficult to meet the costs of multiple verification processes.

The UIDAI - evolving an approach to identity

Under this head, the document points out that the Unique Identification Authority of India (UIDAI) was established in February 2009, attached to Planning Commission. The purpose of the UIDAI is to issue a unique identification number (UID) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives.

The document further gives some important features of the UIDAI model. These are:

- The Unique Identification Numbers (UID) will provide a person's demographic and biometric information and will only guarantee identity, not rights, benefits or entitlement, and citizenship.
- The UIDAI envisions full enrolment of residents focusing on enrolling India's poor and underprivileged communities. This method of authentication will also improve service delivery for the poor.
- Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this, the Authority plans to enroll residents into its database with proper verification of their

demographic and biometric information. The Authority will ensure that the Know Your Resident (KYR) don't become a barrier for enrolling the poor.

- The UIDAI will be the regulatory authority managing a Central ID Data Repository (CIDR), which will issue UID numbers, update resident information, and authenticate the identity of residents as required. In addition, the Authority will partner with agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI. The Authority will also partner with service providers authentication.
- The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR verification, collecting demographic data on residents for their specific requirements, and in authentication.
- Enrollment will not be mandated. The UIDAI approach will be a demand-driven one, where the benefits and services that are linked to the UID will ensure demand for the number.
- The Authority's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar.
- Loading intelligence into identity numbers makes them susceptible to fraud and theft. UID will be a random number.
- The Authority will only collect basic information on the resident.
- Registrars will send the applicant's data to the CIDR for the de-duplication.
- The Authority will offer a strong form of on-line authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database.

As far as benefits are concerned, the document says that the UDI will become the single source of identity verification and the resident can use the number multiple times and would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services. The UDI will facilitate the opportunity for the poor and underprivileged residents to avail service provided by the government and the private sector. It will also give migrants mobility of identity.

The UIDAI will help the Registrars and enrollers clean out duplicates from their database, enabling significant efficiencies and cost savings and will also enable them to broaden their reach into groups that till now, have been difficult to authenticate. Eliminating duplication under various schemes is expected to save the government exchequer upwards of Rs. 20,000 crores a year.

The Authority will charge a fee for its authentication services and the Registrars and service providers will also be able to charge for the cards they issue residents with the UID number within UIDAI guidelines.

The UIDAI will start issuing UIDs in 12-18 months, and the Authority plans to cover 6oo million people within four years from the start of the project.

The document further says that India will be the first country to implement a biometric-based unique ID system for its residents on such large scale. It will give the government a clear view of India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments, track money and resource flows across the country.

Under UIDAI Approach, the document says that in 2007, the Planning Commission had recommended an approach to issuing unique identification numbers, where the enrolment into a Unique Identification database could be speeded up by using existing resident records in the databases of the Election Commission, PAN etc.

Under the title **- The structure of the UIDAI**, the document points out that the UIDAI, as a statutory body, will be responsible for creating, administrating and enforcing policy. The UIDAI will also design and create the institutional microstructure to effectively implement the policy. This will include a Central ID Data Repository (CIDR), which will manage the central system, and a network of Registrars who will establish resident touch points through Enrolling Agencies. It will store resident records, issue unique identification numbers, and verify, authenticate and amend resident data.

The CIDR will only hold the minimum information required to identify the resident and ensure no duplicates. This will include:

i)Unique Identity Number

The document points out that The UID will be a random numeric that is unique across all residents in India. In older identity systems, it was customary to load the ID number with information related to the date of birth, as well as the location of the person. However this makes the number susceptible to fraud and theft, and migration of the resident quickly makes location details out of date.

ii) Identity Fields: The fields associated with the UID number will be:

- Name
- Date of Birth
- Gender
- Father's Name
- Father's UID number (optional for adult residents)
- Mother's Name
- Mother's UID number (optional for adult residents)
- Address (permanent and present)
- Expiry date
- Photograph
- Finger prints

The UIDAI will partner with variety of agencies and service providers including central and state government agencies such as Oil Ministry and LIC and private sector participants such as banks and insurance firms to enroll residents for UID numbers and verify their identity. The UIDAI will enter into agreement with individual Registrars of the agencies, and enable their on-boarding into UID system.

Under the heading **Enrolment into the UID**, the document says that a critical aspect of the UID enrolment process is that enrolment will not be through a mandate, but will be demand driven. The basic advantage of the UID that can drive this demand, which is to be communicated while promoting enrollment, is that the UID will be **one number, which can be used to prove identity for life**. Once the resident gets this unique ID, it may be accepted as identity proof across service providers. Once the UID number is assigned, the Authority will forward the resident a letter which contains his/her registered demographic and biometric details. If there are any mistakes in the demographic details, the resident can contact the relevant Registrar/enrolling agency within 15 days. The letter that UIDAI sends to resident will consequently contain all demographic details in English as well as the local language of the state in which the resident resides.

The UID enrolment strategy in rural and urban India

The document says that the approach of the UIDAI to enrolment will be a **pro-poor/pro-rural one**.

The Registrars targeted for rural India--- the NREGA, PDS and RSBY- will be government agencies with large rural networks and significant bases among the poor. The enrolment strategy for urban India will include organizations which will dominate services for urban residents, such as LIC and Passport. In addition, the UIDAI will also partner with the Registrar General of India (RGI) --who will prepare the National Population Register through the Census 2011 to reach as many residents as possible and enroll them into the UID database. This may require incorporating some additional procedures into the RGI data collection mechanism, in order to make it UID-ready.

A focused effort to enroll the poor and hard to reach groups

The document further points out that while the UIDAI intends to target Registrars that have large networks among the poor and rural communities in India, it will also emphasize multiple approaches to reach specific, frequently marginalized groups. The urban poor who are mainly of migrant workers with temporary or seasonal jobs are among the most ignored and disadvantaged people in India. The following may be ways to get them enrolled into the UID system.

Co-resident enrolment: Many of India's urban poor work as drivers, maids, or as workers associated with a family or a business. One approach to reach them could be for the head of family or business to enable these members to get enrolled into the UID with the same address proof the family or business usage.

Financial Institutions: The urban poor often borrow from micro-finance institutions and other sources and these could serve as enrolment points for them.

NGOs and Non-profits: Several established Non-profits working in urban slums in education, healthcare and social empowerment can be used to help endorse identity for people who lack documentation.

Children: India is a country with over 400 million residents below the age of 18 who need to be specifically targeted. ICDS is one of the world's largest integrated early childhood programmes, with over 40,000 centres nationwide. These centres can be information or enrolment points for non-school going children.

School admission may be mandated that at the time of joining school it is necessary for children to have a UID or to enroll for one. The SSA programme could also help enroll children in the 6-14 age group into the UID.

Women: Apart from enrollers that are family-based government services in both urban and rural India such as PDS, RSBY etc, there need to be a strategy to cover women outside this net. Financial institutions like micro-finance institutions and self-help groups across the country, Organizations like Mahila Samakhya, and The National Commission for Women can be important enrolment points for women.

Differently-abled people: The document points out that India has over 60 million differently-abled people, and identity for this population is a massive challenge. Organizations like National Centre for Promotion of Employment for Disabled People (NCPEDP), NGOs and Rights Groups associated with NCPEDP would be good mechanisms to reach out to this section of the population for enrolment.

Tribals: India has approximately 90 million tribals. The government has many programmes for the 697 notified tribes, which can be used for enrolment and information dissemination. In addition, NGOs and government in states with high tribal populations can be Registrars for tribal groups.

The document further talks about the cost of the cards, its clean enrolment, and updating of UID details. It says that based on initial estimate, the enrolment of each resident may cost between RS. 20 and Rs. 25, leading to a potential total enrolment cost of Rs. 3000 crore. The Registrars have the option of charging for the cards they issue residents to offset enrolment costs. The UIDAI may issue guidelines around such pricing.

In this context, the UIDAI will periodically carry out a process audit of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI. The audit might focus on 1) verification against scanned documents, 2) Physical document Verification, 3) Periodic process audits.

The document says that the UID number is a lifetime number, but the biometric information contained in the central database will have to be regularly updated. Children may have to update their biometric information every five years, while adults update their information every ten years as from time to time, the demographic information that CIDR holds on the resident may also become outdated. The Authority expects to start issuing UIDs in 12-18 months, and enrolment for the UID number is expected to reach a critical mass of around 200 million residents in two to three years.

It also says that there are few challenges for full enrolments in registering the approximately 60,000 babies that are born in the country every day. First, since their biometric is not stable, they have to re-scanned at a later age. Second, names are often not given in India at the time of birth registration. Over the next several years, the UIDAI expects to enroll close to the entire Indian population. One way to ensure that the UID number is used by all government and private agencies is by inserting it into the birth certificate of the infant. It is also necessary to record deaths in the country, and the birth and death registration act provides for such registration. The UID system will not remove a record upon the person's death; It will simply mark it as deceased.

Ensuring Strong Authentication, and what it means for the UIDAI

The document points out that the UIDAI approach - which will be online authentication, with biometric check - creates a very strong authentication system, and gives the UIDAI significant ability to confirm an individual's identity.

The speed of UID adoption in India depends on whether the number can help in eliminating poverty and marginalization, and in enabling greater transparency and efficiency in service delivery. If it succeeds in these goals, the number will become indispensible for residents in accessing services. While the UID can provide the strongest form of pre-verification and identity authentication in the country, It cannot ensure that targeted benefit programmes reach intended beneficiaries. The pro-poor impact of the UID, consequently, will not gain traction unless there is a mechanism to link the UID process with actual service delivery.

The document says that there is tremendous value to be gained from widespread adoption of the UID for authentication, especially for residents. While enrolment in the UID database will ensure that residents are not denied access to fundamental services and rights because they cannot present positive proof of identity, adoption in authentication could go one step further, and ensure that residents consistently receive these services. This can include a wide range of benefits such as education, health coverage, old-age pensions and subsidized food grains, thereby fulfilling the UIDAI's pro-poor agenda.

It further says 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 service.

Types of Authentication

The document further says that there are multiple forms of authentication that the UID authority can offer. Certain types of authentication would have low to medium assurances if there is the possibility that the card is forged. Some main forms of authentication are given below. These are:

- Online demographic authentication where the authenticating agency compares the UID number and demographic information of the UID holder to the information stored in the UID database. The assurance level is medium.
- Online biometrics authentication where the biometrics of the UID holder, his UID and key demographic details are compared to the details in the CIDR. The assurance level is high.
- Online demographic/biometric authentication with API where Registrar's backend system makes a programmatic call to the authentication AIPs exposed by the UID system to perform authentication. The assurance level here may be medium-high.
- Photo match authentication where the photo on the card is compared with the cardholder. The assurance level here is low.

Authentication and the UIDAI revenue model

The agencies which request a resident authentication service will have to be registered with the UIDAI and follow strict guidelines in using service as well as in managing resident information.

Basic identity confirmation from the UIDAI would be free. Chargeable authentication services can be of two types:

Address verification: The service provider usually verifies address through a physical visit, as well as an enquiry to confirm the other information provided. This process is expensive and costs between Rs. 100 and Rs. 500 per verification. In the proposed transaction with UID Authority, the agency will submit the UID, name, and address of the resident to the CIDR, which will confirm the address. As a result, the agency will not have to do physical address verification.

Biometric confirmation: Service such as issuing a credit card or granting a loan need a photograph along with other documents for the confirmation of the resident's identity. In the proposed transaction with the UID Authority, the agency can send the scanned photograph or fingerprint together with other demographic details to confirm the identity of the person.

Under the title **Legal Framework**, the document says that the Constitution of India, through Directive Principles of State Policy mandates that the State strive to minimize inequalities of income and endeavor to eliminate inequalities in status amongst individuals. It is therefore, imperative to have a proper legal structure in place to ensure the smooth functioning of the UIDAI. This section provides an overview of the legal and policy framework.

The document says that the law will contain a prescription against collecting any other information than the information permitted, with prohibitions against collection of information regarding religion, caste, race, ethnicity and other similar matters.

- To verify the identity of any person at the time of the provision of information, the issuance of a Unique Identity Number.
- To permit the UIDAI to set up or facilitate the infrastructure by which third parties can authenticate the identity of persons who have provided information to the UIDAI and the circumstances and conditions they can seek such verification
- To establish or appoint a Central ID Data Repository (CIDR) for the purposes of collecting, managing and securing the database and to outsource any such functions.
- To permit the appointment of Registrars and other service providers in accordance with criteria laid down by the UIDAI to enroll people that seek unique identity numbers directly or indirectly through enrolling agencies.
- To prescribe regulations for the regulation and functioning of the CIDR, Registrars, enrolling agencies and other service providers.
- To call for information and records, conduct inspections, inquiries and audit of the CIDR, Registrars, enrolling agencies and service providers.
- To hire the necessary technical and professional personnel necessary for executing the mandate and fulfill the objectives of the UIDAI.

The law will also contain:

- Penal provisions against persons employed by, or associated directly or indirectly with, the CIDR, Registrars, enrolling agencies and other service providers for failing to comply with the directions issued under the Act.
- Penal provision for persons who intentionally or fraudulently provide wrong information, attempt to obtain a second unique identity number, steal the identity of any living or dead person, etc.

Protecting privacy and confidentiality

The UIDAI will protect the right to privacy of the person seeking the unique identity number. The information on the database will be used only to authenticate identity. In order to protect the right to privacy and confidentiality the UIDAI will do the following:

- UIDAI will enter into contracts with Registrars to ensure confidentiality of the information they collect through the enrolling agencies.
- UIDAI will set in place protocols for information gathering and storage to be followed by the Registrars and enrolling agencies.

Offences under the UIDAI Act

The UID database will be susceptible to attacks and leaks at various levels. The UIDAI must have enough courage to be able to deal with these issues effectively. It will be an offence under the UIDAI Act to engage in the following activities:

- Unauthorized disclosure of information by anyone in the UIDAI, Registrars or Enrolling agencies.

- Sharing any of the data on the database with anyone.
- Engaging in or facilitating analysis of the data for anyone.
- All offences under the Information Technology Act shall be deemed to be offences under the UIDAI if directed against the UIDAI or its database.

Data Security and Fraud

The document, under this title, points out that even as the UIDAI stores resident information and confirms identity to authenticating agencies, it will have to ensure the security and privacy of such information.

It says that the UIDAI envisions storing basic personal information, as well as certain biometrics. However, limiting its scope to this, and not linking this information to financial/other details does not make the resident records in the database non-sensitive. Biometric information for example, is often linked to banking, social security and passport records. Basic personal information such as date of birth is used to verify owners of credit card/bank accounts and online accounts. Such information will therefore, have to be protected. Loss of this information risks the resident's financial and other assets, as well as reputation, when the resident is a victim of identity theft.

Fraud Scenarios

Since the CIDR will store the biometric of residents, identity fraud will be easier to control. The only form of fraud that may go undetected in the UID system is if a person registers his/her details and biometrics under an entirely different name, with forged supporting documents.

.Project Risk

The document in the end says that the UID project does face certain risks in its implementation. Some of these risks include:

1. **Adoption risks:** There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and poor) the number will not be successful in the long run.
2. **Political risks:** The UID project will require support from state governments across India. The project will also require sufficient support from individual government departments, especially in linking public services to the UID, and from service providers joining as Registrars.
3. **Enrolment risks:** The project will have to be carefully designed to address risks of low enrolment - such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities-as well as managing difficulties in address verification, name standards, lack of information on date of birth, and hard to record fingerprints.
4. **Risks of scale:** The project will have to handle records that approach one billion in number. This creates significant biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.
5. **Technology risks:** The authority will have to address the risks carefully - by choosing the right technology in the architecture, biometric, and data management tools.
6. **Privacy and security risks:** The UIDAI will have to ensure that resident data is not shared or compromised.

The Identity Project Report : An assessment of the UK Identity Cards Bill and its Implications

Hosted and Published By:

London School of Economics (LSE), The Department of Information System

June 27, 2005

Bird's Eyeview

This report is a lengthy document containing 303 pages. Talking about the development of the report, the document says that on 29 November 2004, the government published the National Identity Cards Bill. As the Bill passed through Parliament, there was increasing concern within business, academia and civil liberties groups about the lack of informed public debate about its implications for the United Kingdom. As the Information Commissioner told The Times newspaper in August 2004:

"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with."

In persons to that concern, in January 2005 the London School of Economics (LSE) initiated a project to examine in detail the potential impacts and benefits of the Identity Cards Bill. The objectives of the project are to:

- Provoke debate about the nature and impact of the National Identity Scheme;
- Gather a broad spectrum of opinions from diverse stakeholder groups;
- Consider possible architectures for delivering the infrastructure;
- Interpret the proposed legislation and debate its implication;
- Publish a detailed report that explores the key issues and recommends changes to the Government's plans where necessary;
- Establish a working party that will continue to consider identity issues after the publication of the report.

Work on the project began in January 2005.

The principles outlined in this report are derived from the recommendations of Expert Panels representing business, government, academia, non-government organizations and industry/professional bodies. These groups have met on several occasions to debate the impact of the Identity Cards scheme. Further input has been obtained through one-to-one meetings, documents submitted by Expert Panel members, and the ongoing debate within the project team.

The Expert Panel findings supported the principle and objectives of the Identity Cards Bill, but recommended numerous changes to the system architecture, development and management.

The LSE project team has developed the Expert Panel recommendations into the broader analysis and recommendations in this report. The team has solicited opinions, analysis and criticisms from a large group of industry and academic specialists covering technology, security, privacy, public sector, procurement and legal disciplines.

The LSE team has made several attempts to engage the Home Office Identity Cards Unit in the project, but at the time of publication there has been no meeting between the two parties.

Overview

The report assesses the implications, costs, opportunities and consequences arising from current legislative proposals to introduce a National Identity Cards Scheme. This report is based on research of available evidence. It does not deal with principle or speculation.

The report says that the goals of combating terrorism, reducing crime and illegal working, reducing fraud and strengthening national security are the concerns of the government, but the report challenges assumptions that an identity card system is an appropriate, safe and cost-effective way to achieve those goals.

The report concludes that the establishment of a secure national identity system has the potential to create significant, though limited, benefits for society. However, the proposals currently being considered by Parliament are neither safe nor appropriate. There was an overwhelming view expressed by stakeholders, experts and researchers involved in this report that the proposals are too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence. The report further says that the current proposals miss key opportunities to establish a secure, trusted and cost-effective identity system.

There is no evidence to support the use of identity fraud as a justification for the current identity card model. Many of the claims made about the prevalence of identity fraud are without foundation. A card system such as the one proposed in the Bill may even lead to a greater incidence of identity fraud.

The concept of a national identity system is supportable, but the current proposals are not feasible. The report therefore outlines an alternative model for an identity card scheme that will achieve the goals of the legislation more effectively.

Dwelling into the rationale behind the Bill, the report points out that the Government seems intent on pointing to international obligations and precedents to justify the introduction of a national identity card. But the research indicates that a national identity card need not resemble the one that the Government is proposing, nor is any nation under an obligation to create such a card. Indeed no other country has done so with such a pretext.

It further says that an appropriate identity system for the United Kingdom would be one based on a foundation of public trust and user demand rather than one based on enforcement through criminal and civil penalties. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies and the creation of a more flexible "citizen centred" model.

The report here outlines some key areas of concern with the proposals made not in the Bill. The areas are:

Purposes of the system

The report says that proposals seem to address multiple, divergent goals, yet the evidence from other national schemes indicate that identity systems perform best when established for clear and focused purposes. The goal of 'prevention and detention of crime', for example, involves a potentially huge number of applications and functions that may not be appropriate for an identity system that also seeks to achieve a goal of public services delivery. Preventing identity fraud 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.

It may be true that the proposed scheme is likely to have an impact on false identity within the benefits sector. However, benefit fraud through false identity is relatively rare and the cost of introducing an identity card in the benefits environment would far outweigh any savings that could be made.

The Technological Environment

The report states 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. Small and less ambitious systems have encountered substantial technological and operational problems that are likely to be amplified in a large scale national system. The use of biometrics gives rise to particular concern because this technology has never been used at such a scale.

The proposed system unnecessarily introduces, at a national level, a new tier of technological and organizational 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. From a security perspective, the approach to identify verification outlined in the Identity Cards Bill is substantially flawed. 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.

Cost

The report further points out that because of its size and complexity, the identity system will require security measures at a scale that will result in substantially higher implementation and operational costs than has been estimated.

The estimated cost of the ten-year rollout of the proposed identity cards scheme will be between 10.6 billion pound and 19.2 billion pound, with a median of 14.5 billion pound. This figure does not include public and private sector integration costs, nor does it take into account possible cost overruns.

The report says that private sector costs relating to the verification of individuals may account for a sum equal to or greater than the headline cost figure suggested by the government. Staff must be trained to use biometric systems, and in larger organizations must be on hand at all times to verify customers and new employees. New facilities may have to be built to accommodate applicants who feel sensitive about having their biometrics taken in public area.

The Government has substantially underestimated the cost of biometric readers. Because of physical irregularity or mental impairment, a significant number of people are unable to provide a stable biometric unless expensive equipment is used.

The cost of registration of applicants appears to have been underestimated. The Bill makes provision for the disclosure and processing of more than fifty sources of identification. This estimate, coupled with the capture of biometrics and the investigation of the biographical history of applicants may result in registration alone costing more than the projected overall cost of the identity system.

Direct cost to people applying to be registered on the system is also likely to be higher than anticipated. Biometric registration may have to be repeated every five years for much of the population. As people age, their biometric change and become less reliable. As a consequence, these people are more likely to face problems with the use of the identity card system and may require more frequent updates of their biometric information stored on the system.

One possible solution to these problems is the endemic use of multiple biometrics. However, this feature would add significantly to the cost of the system.

The Legal Environment

The report further states that in its current form, the Identity Cards Bill appears to be unsafe in law. A number of elements potentially compromise Article 8 (Privacy) and Article 14 (discrimination) of the European Convention on Human Rights. Because of the difficulty that some individuals may face in registering or verifying their biometrics, there is a potential conflict with national laws such as the Disability Discrimination Act and Race Relation Act.

The proposals appear to be in direct conflict with the DATA Protection Act. Many of these conflicts arise from the creation of a national identity register, which will contain a substantial amount of personal data, some of which would be highly sensitive. The amount of information contained in the register, the purposes for which it can be used, the breadth of organizations that will have access to the Register and the oversight arrangements proposed are contentious aspects.

The compulsory acquisition of fingerprints in passports may violate the common law right to exit and re-enter the UK. This common law right of each UK citizen is now enshrined in the immigration Act, which does provide for exceptions. However, if a right to leave the UK exists and a passport is a pre-requisites, then a right to a passport must exist also, subject to those exceptions. The Act's exceptions are aimed in spirit at immigration control of foreign nationals, not control of UK citizens leaving the country.

The report further points out that the Bill also creates a possible conflict with the right of freedom of movement throughout the EU for EU citizens. It is arguable that the Identity Cards Bill may discourage non-UK EU workers from coming to the UK to work and so many infringe EU principles on the freedom of movement of workers. Further, liability and responsibility for maintaining accuracy of data on the Register, conducting identity checks and ensuring the integrity of the overall operation of the scheme has not been resolved.

Oversight

The oversight arrangements set out in the Bill appear to be inadequate in several key respects. An Identity Cards Commissioner as envisioned by the legislation may be an insufficient mechanism to adequately promote public trust.

The current population of oversight bodies in the UK is complex, inefficient and frequently in conflict.

International Obligation

The Government has consistently asserted that the biometric proposal, both in the new UK passport format and in the identity cards legislation, is a harmonious measure required by international obligation, and is thus no different to the plans and intentions of the UK's international partners. However, the report says that there is no evidence to support this assertion.

The report further says that it has been found that the Government is unnecessarily binding the Identity Cards Scheme to internationally recognized requirements on passport documents. By doing so, the Government has failed to correctly interpret international standards, generating unnecessary costs, using untested technologies and going well beyond the measures adopted in any other country that seek to meet international obligation.

As far as **National Security, Organized Crime and Terrorism** are concerned, the report states that this objective has been subject to claim and counter-claim. It says that the Government's considered position is that an ID card will help in the fight against terrorism. However, the essential facts are disputed.

In 2004, Privacy International published the findings of the only research ever conducted on the relationship between identity cards and terrorism. It found that there was no evidence to support the claim that identity cards combat terrorism. The report further stated that the detailed analysis of information in the public domain in this study has produced no evidence to establish a connection between identity cards and successful anti-terrorism measures.

It says that terrorists have traditionally moved across borders using tourist visas (such as those who were involved in the US terrorist attacks), or they are domicile and are equipped with legitimate identification cards (such as those who carried out Madrid bombing). Of the 25 countries that have been most adversely affected by terrorism since 1986, eighty per cent have national identity cards, one third of which incorporate biometrics. This research was unable to uncover any instance where the presence of an identity card system in those countries was seen as a significant deterrent to terrorist activity.

Only a small fraction of the ninety million crossings into UK each year are supported by comprehensive security and identity checks.

Of equal significance is the admission by the Home Office that visitors to the UK who are entitled to a stay of three months less will not be required to apply for a card.

The Government appears to be incrementally backing away from its original assertion that the card system would be a tool to directly prevent terrorism.

Under the heading of **Biometrics**, the report says that prosecution for dealing with or creating false ID cards and high-level identity documents have been pursued in many countries, including Britain, Hong Kong, Pakistan, Ireland, Malaysia, Yemen, Czech Republic, Venezuela, India, Italy, and Sri Lanka where the forgeries were supplied by suicide bombers.

In many cases the false identity was secured merely by bribing an official or by providing counterfeit documentations at the point of registration. Through the Bill, the government proposes to eliminate this risk by establishing a "clean" database of identities. Entry onto the database will require multiple biometric captures, biographical footprint checking and a range of primary documentation.

A biometric is a measure of identity based on a body part or behavior of an individual. The most well known biometrics are fingerprints, iris scans, facial images, DNA and signatures.

The report also says that in the UK identity proposals, biometrics would be taken upon application for a card and entry on the National Identification Register, and would be used thereafter for major events such as obtaining license, passport, bank account, benefits or employment.

The Government has repeatedly claimed that the use of biometrics will prevent any fraudulent use of the system.

However, any claim of infallibility is incorrect. All biometrics have successfully been spoofed or attacked by researchers. Substantial work has been undertaken to establish the technique of forging or counterfeiting fingerprints while researchers in Germany have established that iris recognition is vulnerable to simple forgery.

The report also points out that a 2002 report of the United States General Accounting Office "using biometrics for border security" states that biometrics technologies are maturing but are still not widespread or pervasive because of performance issues, including accuracy, the lack of application-dependent evaluations, their potential susceptibility to deception, the lack of standards, and questions of users' acceptance. It also warns making assumptions about the ability of the technology to perform across large populations.

There are two distinctive problems that can result from failure to adequately register with a biometric device. The first is described as the Failure to Enroll Rate (FTER). This occurs when a person's biometric is either unrecognizable, or when it is not of a sufficiently high standard for the machine to make a judgment. The second crucial indicator is the False Non-Match Rate (FNMR) that occurs when a subsequent reading does not properly match the properly enrolled biometric relating to that individual.

In this context, the report further points out that fingerprint recognition is in use in a number of cases and is a relative success. Issues with fingerprint recognition include the high rate of false non-match results and social inclusion given that in the current UK population approximately one in a thousand people are unable to provide the required four suitable fingerprints.

Around one in ten thousand people do not have a suitable iris for recognition. Facial recognition is not currently sufficiently reliable for the identification of each member of the population and recent trials have shown relatively poor identification performance.

A small percentage of people, nevertheless amounting to tens of thousands for a national ID cards, are unable to enroll fingerprints or iris images. Ability to recognize both characteristics is known to decline with age. There has been no scientific study to determine the stability of biometric characteristics over time. Apart from ageing, fingerprints may become unrecognizable because of cuts or burns, extreme weight gain or loss.

The report further points out that according to one expert, the understanding of fingerprints is dangerously flawed and risks causing miscarriages of justice. Amongst the numerous fingerprinting that of Brandon Mayfield is indicative of the many problems in assessment and interpretation of fingerprint data. When Mayfield's personal information was combined with the crime scene evidence, the FBI was convinced of his culpability. Yet according to a panel of experts, they were wrong. As the collection of biometric information increases and as it moves from law enforcement to civilian application, the error rate may significantly increase.

The report says that iris recognition is a relatively new identification technique. Nearly all technical reports and trials have been conducted at a general level. It appears that no trials have been undertaken with specific reference to blind and visually impaired trials users. They are frequently excluded from research trials.

The report also states that a 2002 technology assessment report by U.S. General Accounting Office (GAO) highlighted a number of problems with the accuracy of iris recognition. While acknowledging that the mathematics of the technique appeared sound, the enrolment and verification elements of iris recognition were far from perfect. The Failure to Enroll Rate was around half a percent, while false Non-Match rate ranged from 1.9 to 6 percent. This means that around 1:200 of the research population could not enroll, while a further 1: 18 to 1:50 could not match their enrolled iris.

Under the section of **Security, safety and the National Identity Register**, it has been said that from a security perspective, the approach to identity verification outlined in the Identity Card Bill is substantially flawed. This section highlights the reasons for having arrived at the conclusion that the National Identity Register poses a far larger risk to the safety and security of UK citizens than any of the problems that it purports to solve.

It further says that most experienced systems designers will immediately recognize that the combination of requirements poses an extreme challenge even without the security requirements. Even if the security requirements are undertaken the system becomes infeasible unless substantial pruning and simplification is undertaken.

The following sections consider security and safety aspects of the proposal and some of the dilemma that will be faced if a system of this scale and complexity is pursued.

Secure Information System

The report points out that the basic principle used is that if a computer system faces higher security risks, it will need to be of higher security quality in order to counter them. Systems of the character of the National Identity Register (NIR) are large, complex systems which face high levels of security risk because of their connections to other computer and internets.

The NIR is an example of computer systems requiring 'Mandatory Access Control', which means that the security policy cannot be overridden by the users. Although, they are technically feasible on a small scale, experience shows that their development is extremely costly, their performance is very often disappointing and their maintenance and support costs are prohibitively high. The report supports its observation by quoting a US Computer Security Expert DR. Rick Smith:

" Multilevel Security (MLS) systems have rarely provided the degree of security desired by their most demanding customers in the military services, intelligence organizations, and related agencies. The high costs associated with developing MLS products, combined with the limited size of the user community, have also prevented MLS capabilities from appearing in commercial products."

The report says since the NIR will require a mandatory access control system, the scale, complexity and assurance of which is a long way beyond anything ever previously contemplated, the programme is certain to face technical problems of a kind that are known to lead to development difficulties, and very often to uncontrolled cost growth during development.

It thus concludes that there is very good evidence to suggest that it will not be feasible to build a computer system capable of operating the National Identity Register with effective security provisions. An attempt to build a system is likely to be extremely expensive and at high risk of failure.

Enrolment

Talking about the enrolment aspect, the report says that the enrolment stage, in which people's biometrics are recorded and their details entered into the National Identity Register, is critical if the authenticity of each identity record is to be ensured. For example, to make enrolment easy, there will need to be many locations where enrolment is possible. But if there are many locations, the staff costs will be very large and the ability of systems managers to maintain control over the integrity of operations will be degraded.

The integrity of the NIR will be compromised even if only a small number of these thousands of staff act improperly. With smaller centres, in particular, it will become feasible for those who see value in attacking the system to plan an infiltration strategy based on subverting a single enrolment centre. This will add to the requirements for vetting, auditing and other measures designed to ensure that such strategies cannot succeed. This will further increase both the initial and the operating costs.

It also seems likely that such pressures will promote other enrolment strategies involving fewer centres. However, this is unlikely to make significant cost savings since it will simply shift costs onto those who now have to travel some distance in order to enroll. This will also make enrolment much less convenient, adding significantly to the difficulties faced by those who have to register for ID cards. One may expect particular problems for the elderly, for people with physical and mental disabilities, and for people living in remote communities.

Multiple Registrations

The report points out that a key aspect of Government claims about ID is the assertion that it will not be possible for the same person to register more than once with different details, since biometric will expose attempts to achieve this. However, this assertion should be treated cautiously because it depends on several assumptions that have yet to be proven.

Firstly, this assumes a perfect biometric system, whereas it is far from clear that biometrics can meet this challenge for a population of over 50 million people. Secondly, this also assumes that the system as a whole is perfect and will not contain security weaknesses that can be exploited to create multiple registrations containing the same biometrics.

But the report says that one can expect technical attacks, whereby people try to create false identities using rubber finger covers, printed contact lenses and so on. But it is not 'normal cases' that are the source of most problems in secure systems; rather, it is usual one of the many 'special cases' that is exploited to subvert security because the insiders will quickly get to know the 'special cases' and will be sufficiently resourceful to recognize how they can be exploited. It is inevitable that this sort of information filter out to those who want to subvert the system.

The basic problem here is easy to understand: the greater the number of people, who know a secret, the less secret it is. A system such as the National Identity Register, involving thousands of staff, stands little chance of being highly secure.

Identity Verification

The reports says that if ID cards are to be more reliable than 'photo ID' cards, it is essential that their biometric features are widely used with frequent checks against the NIR. Additionally, since the government proposes to hold identity-related data in NIR, on-line identity checks will be essential in key circumstances when access to this date is needed.

This puts the NIR at the heart of the system, which in turn makes the security of NIR data and control of access to it absolutely critical for the safety and security of all who are identified in its records.

The Unique ID Project in India: A Skeptical Note

By:

R. Ramakumar
Associate Professor
School of Social Sciences,
Tata institute of Social Science, Mumbai
August 2010

Bird's Eyeview

In this note, Ramakumar has discussed certain social and ethical aspects of national project to supply Unique ID (UID) numbers to Indian residents. The UID project is being presented by the Indian Government, as a "technology-based solution" that would change the face of governance in India. The writer argues that the UID project would actually lead to the violation of large number of freedoms of Indian people.

While introducing this 15-page note the author points out that 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 imaginaries 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. 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. In the study of e-governance initiatives as well as projects that involve intensive utilization of ICT, social scientists try to emphasis the study of society itself as a starting point. Yet, notwithstanding 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.

The Unique ID (UID) project in India

The note says that 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. The UIDAI is envisaged to enroll all Indian residents into a centralized database, along with their demographic and biometric information.

Further, it is argued by the UIDAI that a clear identity number would transform the delivery of social welfare programmes 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.

The writer argues that thus 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. 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 1990 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. 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. 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". According to 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".

The note further says that besides the above mentioned claims, Nandan Nilekani has also argued that the UID would make it possible to open a bank account in India with no supporting documents, thus expanding "financial inclusion"; the UID would ensure that the public food distribution system (PDS) in India would cease to be wasteful; it would eliminate corruption from the National Employment Guarantee Scheme (NREGS); it would also help ensure and monitor attendance of teachers in schools. Overall, the UID project is presented as a "technology-based solution" that would change the face of governance in India.

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.

But the author says that the UID project is being presented as a tool of good governance but would actually lead to the violation of a large number of freedoms of Indian people. He says that no amount of assertion vis-à-vis improved service delivery can justify the violation of citizen's freedoms and liberties. Next he argues 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, he says that no detailed cost-benefit analysis of the project has been carried out yet. Finally, he argues that the roots of inefficiency in public welfare schemes in India do not lie in the absence of identity proofs. The writer says that he has based his arguments on the literature on the experiences of more modern nations of the world in providing people with unique ID cards and numbers.

Privacy and Civil Liberties

The note says that the 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 variety of purposes. 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. Legislation on privacy cannot be satisfactory guarantees against the possibilities of misuse of ID cards or numbers.

Learning from Western Experiences

Australia was one of the first countries to try the implementation of national ID cards scheme in the recent years. In 1986, the Australian government introduced a Bill in the parliament to legalize the issue of national ID cards in order 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.

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 withdraws 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. 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.

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

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. 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. 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.

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 forced the Labour government to shelve the policy.

The note further says that 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 created 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 note says that 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 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.

The note further says that 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. 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.

For 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 entitlement 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 out sourced to other users, who would in turn, build up their smart card based application (GoI,2007 p.2). 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).

The note says that the 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 Hospital 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. 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. 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.

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.

Technological Determinism in Addressing Social Problems

The note points out that the fact that the UIDAI project in India 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.

Among all the technological features of the UID project, it is the collection and storage of biometric information of residents that is most significant.

In this context, the note says that for a country with more than a billion residents, the sheer scale of the envisaged project is mind-blogging. As per estimates, there are about half a million public distribution outlets in India; there is about 265,000 gram panchayats 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. The crucial question arises here 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? What are the probabilities of system failures of different degrees? What are the "social" costs of these errors? No clear answers are available for these important questions.

The use of Biometrics

The note says that 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. 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", with a completely new identity. 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 UID project would be used for policing purposes. Firstly, regular use of biometric data in policing can lead to a large number of human rights violations. Secondly, 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.

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) that means the 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" of NREGS.

The note, in this context, points out that 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, the fingerprints of manual laboures are highly likely to be broken or eroded, inviting frequent negative responses during validation at the site of wage payments. Globally, fingerprints of about 2 to 5 percent of the population are permanently damaged to the extent that they can not be recorded in the first place. According to some estimates, in developing country like India, the share of persons with bad data could go upto 15 per cent. 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.

The Unknown Costs of the UID Project

The note points out that 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 dollar). 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". 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 case of UK, the LSE group estimated that the costs would lie between 10.6 billion pound and 16.2 billion pound, excluding public and private sector integration costs. This was considerably higher than the estimate of the UK government.

The Efficiency of Social Sector Schemes

The note poses the question would the UID result in an increase in the efficiency of government's poverty alleviation schemes? It says that according to the Chairman of UIDAI, the UID will help address the widespread embezzlement that affects subsidies and poverty alleviation programmes. It says that 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 UIDAI is introduced. The reason is that the premise of the claim made by UIDAI is itself erroneous. The poor efficiency of the 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. This can be well observed in the illustration of the Public Distribution System (PDS) that supplies subsidized food grains to the people.

The case of the PDS

The note here says that 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 leakage 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 (Below Poverty Line) 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 (Above Poverty Line) 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. 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.

Concluding Notes

In conclusion, the note says that 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.

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

A Unique Identity Bill

By:

Usha Ramanathan

An independent law researcher

Published in

Economic & Political Weekly

July 24, 2010

Bird’s Eyeview

In this four and half page commentary the writer talks about the social aspects of India's Unique Identification UID) number project.

It says that India's Unique Identification number project has been sold on the promise that it will make every citizen, the poor in particular, visible to the State. But the UID project raises crucial issues relating to profiling, tracking and surveillance, and it may well facilitate a dramatic change in the relationship between the State and the people. The Unique Identification Authority of India has not acknowledged these concerns so far. And now, nowhere in the proposed draft bill that it has prepared have these issues been addressed, nor have clauses been drafted to prevent abuse of information that will be collected by the agency. With so many questions on the project - regarding biometrics, security and privacy - yet to be answered, it is far from time for parliamentary approval. The writer says that it has been observed that the Constitution is expected to provide the citizen with dignity and privacy; but these missing in the UID project.

She further says that the project pegs its legitimacy on what it will do for poor. The UID number is expected to plug leakages, including Public Distribution System (PDS), ease payments to be made under the National Rural Employment Guarantee Scheme (NREGS), and enable achievement of targets in consonance with the right to education. Service delivery is a central theme in its promotional literature. The raising of expectations is, however, tempered by a quick caveat that the "UID number will only guarantee identity, not rights, benefits, or entitlement.

The UID database is intended to hold information including the names, addresses and biometrics of the person. It has been reiterated with remarkable regularity that the UIDAI will not be gathering information that could lead to profiling. So, religion, caste, language and income, for instance, will not be brought on to the UID database.

The writer points out that the UID has strained every nerve to explain that it will not be a database from which others may derive information about any person. The UIDAI has said that getting on to the UID database is voluntary. That is, it is clarified, there will be no compulsion from the UIDAI. But, she draws the attention to UIDAI's proposition that if other agencies make the UID number essential in their transactions, that is a different matter. In this connection what is to be noted is the fact that the UIAID has been signing memoranda of understanding (MoU) with a range of agencies including banks, state governments and the Life Insurance Corporation of India (LIC) to be "registrars", who then may insist that their customers enroll on the UID to receive continued service.

The commentary also points out that given the dramatic changes that the UID could bring to the relationship between the State and the people, it should cause concern that there has been so little public debate around the UID. There is an unquestioned benignness that is being attributed to the project, which could be explained in part by the image of Nandan Nilekani, whose silence to the project could foster a sense that this is a project around technology, and not about identity. The rhetoric has stayed focused on the poor, which has lent the project legitimacy and there has been no discussion from within the establishment on the possible downsides.

The writer says that one concern that has been raised consistently is on the question of privacy - that information held in a central repository could result in breaches of privacy. The invasion of privacy that technology has facilitated and routine in recent years has eroded the relevance of traditional notions of privacy.

Under the sub-title of " National Security", the writer points out that surveillance is a concern, and a term that is missing altogether in the UIDAI documents.

The writer says that there are three initiatives that, together, form a pattern that is disturbing. The UID only produces a number which is a tag that is poised to be 'universal' and 'ubiquitous'. Its capacity to link disparate pieces of information is difficult to dispute. Place this in the context of the National Intelligence Grid (NATGRID), and the Home Minister P. Chidambaram's statement begins to sound ominous. " Under NATGRID", he is reported as having said, "21 sets of databases will be networked to achieve quick seamless and secure access to desired information for intelligence and enforcement agencies" (The Hindu, 14 February 2010). This is to enable them "to detect patterns, track travelers, and identify those who must be watched, investigated, disabled and neutralized". Many of these intelligence agencies, including the Research and Analysis Wing (RAW) and Intelligence Bureau (IB), are neither creatures of the law, nor are they subject to oversight.

In November 2009, newspapers reported Chidambaram's statement that the government would soon be setting up a DNA data bank. There has been no word on the subject since, but on 12 July 2010, the Indian Express carried news of an impatient debate that has erupted about speeding up DNA data banks to hold DNA data of convicts. This is just a stretch away from extending it to more classes of the population.

The introduction to the UID has been in terms of investing every resident with an identity, as a single stop for authentication identity, as a de-duplication exercise, for plugging leakages, as a tracking device, and as a wage transferring device. There are, however, other concerns that have been voiced and which remain unresolved.

In the rest of the paper the writer talks about these unresolved concerns like the context of convergence, the national population register (NPR), and the shaky edifice of biometrics on which this superstructure is being built. These have been already discussed in the previous documents.

Infopack

Popular Information Centre

peaceact@bol.net.in

peaceact@vsnl.com

Phone & Fax:
(011) 2685 8940
(011) 2696 8121

If Undelivered, please return to:

Infopack

A-124/6 (2nd Floor), Katwaria Sarai, New Delhi 110 016

Telefax : 26968121 & 26858940 # E-mail : peaceact@bol.net.in & peaceact@vsnl.com