

IN THE HIGH COURT OF JUDICATURE AT BOMBAY
ORDINARY ORIGINAL CIVIL JURISDICTION
PUBLIC INTEREST LITIGATION NO. 152 OF 2013
Vickram Crishna & Ors. .. Petitioners

Versus

(L) 10/12

Unique Identification Authority
of India & Ors. ..

Respondents

INDEX

PART - I

| <u>Sr.No.</u> | <u>Particulars and Dates</u> | <u>Pages</u> |
|---------------|--|--------------|
| 1. | Proforma | A to C |
| 2. | Synopsis | D to F |
| 3. | Petition | 1 to 55 |
| 4. | Vakalatnama | 56 to 61 |
| 5. | Memorandum of Registered Address of Petitioners | 62 |
| 6. | List of Documents | 63 |
| 7. | <u>Exhibit "A"</u> Copy of the aforesaid letter dated | 64 to 70 |
| 8. | <u>Exhibit "B"</u> Copy of the Application Form | 71 |
| 9. | <u>Exhibit "C"</u> Copy of the UID Strategy Overview dated April 2010 issued Respondent No.1. | 72 to 115 |
| 10. | <u>Exhibit "D"</u> Copy of UID for Dummies" authored by Simi Chacko and Pratiksha Khanduri dated 12 th September 2011. | 116 to 156 |

PART-II

| | | |
|-----|--|------------|
| 11. | <u>Exhibit "E"</u> Copy of the recommendations dated 04 November 2008. | 157 to 165 |
| 12. | <u>Exhibit "F"</u> Copy of the Notification dated 28 th January 2009 | 166 to 168 |
| 13. | <u>Exhibit "G"</u> Copy of the notification appointing Nandan M. Nilekani as chairman | 169 to 173 |
| 14. | <u>Exhibit "H"</u> Copy of central identity databases facilitate the reverse | 174 to 250 |
| 15. | <u>Exhibit "I"</u> Copy of the report | 251 to 282 |
| 16. | <u>Exhibit "J"</u> Copy of the UK ID cards system | 283 to 294 |
| 17. | <u>Exhibit "K"</u> Copy of the UIDA Bill | 295 to 326 |

PART-III

| | | |
|-----|--|------------|
| 18. | <u>Exhibit "L"</u> Copy o the Unique Identity Bill" by Prof. Usha Ramanathan, a prominent advocate on the right to privacy in India. | 327 to 331 |
| 19. | <u>Exhibit "M"</u> Copy of the detailed report Of the Standing Committee dated 13 th December 2011. | 332 to 379 |
| 20. | <u>Exhibit "N"</u> Copy of recent news report of theft and sale of enrolment data from private agencies in Punjab. | 380 |
| 21. | <u>Exhibit "O"</u> Copy of the Edgar Whitley interview printed in Frontline Affidavit in support. | 381 to 384 |
| 22. | <u>Exhibit "P"</u> Copies of detailed reports, analysis and studies conducted on the efficacy of UIDAI to address welfare distribution issues conducted and written by Prof. Reetika Khera. | 385 to 391 |
| 23. | <u>Exhibit "Q"</u> Copy of the 4G Solutions Report | 392 to 400 |
| 24. | <u>Exhibit "R"</u> Copy of the Biometrics Standards Committee report commissioned by the UIDAI. | 401 to 457 |
| 25. | <u>Exhibit "S"</u> Copy of the circular | 458 to 466 |
| 26. | <u>Exhibit "T"</u> Copy of Circular | 467 to 484 |
| 27. | Affidavit in support | 485 to 486 |
| 28. | Advocate Certificate | 487 |

2/H

IN THE HIGH COURT OF JUDICATURE AT BOMBAY
ORDINARY ORIGINAL CIVIL JURISDICTION
PUBLIC INTEREST LITIGATION NO. OF 2012

Vickram Crishna & Ors

... Petitioners

Versus

Unique Identification Authority of India & Ors.

...Respondents

SYNOPSIS

| Date | Particulars |
|------------|---|
| 04/12/2006 | An empowered group of Ministers (EGoM) was constituted and the twin proposals to create both a National Population Register by an amendment to the Citizenship Rules and UID were brought into the purview of this empowered group of Ministers (EGoM). |
| 04/11/2008 | The Committee of Secretaries and the Empowered group of Ministers' made recommendations for the constitution of the Unique Identification Authority of India. |
| 28/01/2009 | The Planning Commission notified the recommendations for the constitution of the Unique Identification Authority of India as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. . |
| | The Unique Identity Project (the "UID"), a brainchild of the Planning Commission, was announced with the ambitious agenda of collecting and documenting biometric and other information of the entire Indian population. |

| | |
|------------|---|
| 29/01/2009 | The government came with a notification creating the Unique Identity Authority of India (U.I.D.A.I.), an agency established under the aegis of the Planning Commission to issue Unique Identity Numbers (UID) to every Indian citizen. |
| 23/07/2009 | The Government appointed Shri. Nandan M. Nilekani as Chairman of the Unique Identification Authority of India, in the rank and status of a Cabinet Minister for an initial tenure of five years and Mr. Nilekani has joined the UIDAI as its Chairman on 23/07/2009. |
| 30/07/2009 | An advisory council presided by the Prime Minister was set up on 30 July 2009 to advise the UIDAI on Programme, methodology and implementation to ensure co-ordination between Ministries/Departments, stakeholders and partners. |
| | The declared aim of the <i>aadhaar</i> numbers scheme is to streamline the delivery of services to Indian residents and avoid corruption and misuse of public funds and subsidies. |
| | UIDAI was created through an executive fiat to enable the process of issuing UID cards across India, without any rules, procedures, or guidelines. Its further extension, universalisation and implementation across the nation remains must contingent upon both an initial success together alongwith legislative passage of the proposed National Identification Authority of India Bill, 2010 |
| April 2010 | Unique Identification Authority of India issued a UID Strategy Overview. |

| | |
|------------|---|
| April 2011 | Government of Maharashtra through its GR dated April 2011, plans to make Aadhaar a compulsory requirement for government employees for accessing their salary benefits. |
| 12/09/2011 | A detailed alternative note that critically explains the functioning of the UID titled "UID for Dummies" was authored by Simi Chacko and Pratiksha Khanduri. |
| 26/09/2011 | The Petroleum Ministry has made Aadhaar a mandatory condition for LPG users by a Gazette Notification dated 26/09/2011. |
| 13/12/2011 | The Standing Committee of the Parliament has rejected the present draft of the NIDAI as not meeting the required constitutional standards by a report dated 13/12/2011. |
| | In complete disregard to both, UID numbers without any safeguards against the tremendous breach of privacy entrenched in the scheme as it presently stands are being issued across the country without any legislative framework. |
| | Hence the petition. |

Points to be urged:

1. Whether the UIDAI-Aadhaar scheme as it presently stands as a mere executive fiat, is illegal, arbitrary and unconstitutional by granting wide, unrestricted powers to an unaccountable independent body known as UIDAI, and also to private agencies; leading to huge breaches on the right to privacy and dignity of Indian citizens?
2. Whether reasonable restrictions on fundamental rights can only be through legislative mandate and the UID scheme makes invasion into fundamental rights without a legislative mandate and is hence bad in law?
3. Whether the co-extensive executive power exercised to implement UIDAI can be untrammelled and function towards restricting fundamental rights without any due procedure, guidelines and

4 D

safety mechanism, which can only be ensured through a statutory framework?

4. Whether the mandatory enforcement UIDAI-Aadhaar scheme contravenes Article 21 by restricting the right to decision making, personal integrity, choice and dignity?
5. Whether the impugned notification dated 4th November 2008 is illegal, arbitrary and bad in law for setting out an extensive task of launching UID way beyond the executive competence, without any guidelines, rules and procedure?
6. Whether the impugned notification 4th November 2008 is illegal, arbitrary and unconstitutional and in breach and contravention of Article 14 for assigning the most essential function of data collection via enrolment for Aadhaar to private agencies?
7. Whether the notification 4th November 2008 is further illegal as it delegates excessive powers with the UIDAI without any guidelines or procedure, leading to further unrestricted delegation of powers to private parties creating great potential for data leakages, and breaches of sensitive private data leading to Indian Citizens?
8. Whether this convergence of silos of information will completely abolish the veneer of privacy that protects the daily lives of individuals by the cross-referencing service usage of a particular individual through a single numeric bio-metric identity has huge implications for building State inroads into every private activity and service accessed by that individual, this is further complicated by the possibility of private actors also accessing similar information?
9. Whether the right to privacy as upheld within the right to life in Article 21, and restriction if any must be justified through a rational and reasonable statutory procedure?

Acts and Regulations Relied on:

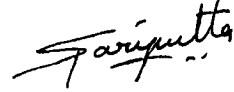
1. Constitution of India

Judgments relied on:

- 1) *Kharak Singh v. State of Uttar Pradesh*
- 2) *Gobind v. State of Madhya Pradesh*
- 3) *PUCL v Union of India* (1997) 1 SCC 301
- 4) *Sharda v Dharampal* (2003) 4 SCC 493
- 5) *R. Rajgopal v. State of Tamil Nadu* (1994) 6 SCC 632

- 6) *Phoolan Devi v. Shekhar Kapur* (57 (1995) DLT 154)
- 7) *Khushwant Singh v. Maneka Gandhi* AIR 2002 Del 58.

Additional judgments will be relied on at the time of argument.



Advocate for the Petitioner

1 /

IN THE HIGH COURT OF JUDICATURE AT BOMBAY
ORDINARY ORIGINAL CIVIL JURISDICTION

PUBLIC INTEREST LITIGATION NO. OF 2012

In the matter of the public
interest of protecting the rights
of privacy, autonomy, dignity
and free and full enjoyment of
life of the citizens of India,
guaranteed under Articles ¹⁴19
and ^{and 22.6}21 of the Indian
Constitution;

AND

In the matter of non-voluntary
and premature implementation
of "Aadhaar" in strict breach of
Article 21 of the Indian
Constitution

AND

In the matter of excessive
delegation of essential function
without any guidelines, rules or
police framework in

2

2

Notification Dated 29th January
2009 creating the UIDAI

AND

In the matter of potential
breaches of the right to privacy
of citizens of India, through the
means of data collection,
storage and sharing by the
UIDAI, without any legitimate
and rational nexus of improving
the public welfare system

AND

In the matter of standing
committee of the Parliament
Report dated 13th December
2010 rejecting the proposed
National Identification
Authority of India Bill, 2010

1. Vickram Crishna, aged 60 yrs,

Residing at A31 Queens Apts,

Pali Hill, Bandra, Mumbai 400050

E mail. vvcrishna@gmail.com

PAN No: AEWPC 2794M

2. Kamayani Bali Mahabal, aged 40 years,

Residing at 503, Juhu Bahart CHS,

Gandhi Gram Road,

Juhu, Mumbai 400 059

Email kamayni@gmail.com

PAN No: AHFPB0195 F

Ph No: 9820749204

3. Yogesh Pawar, aged 43 years,

Residing at 18B/704, Bimbisar Nagar,

Near SRP camp, Western Express Highway,

Goregaon E, Mumbai 65

Email yogeshp1969@gmail.com

PAN No: ALCPP4671 P

4. Dr Nagarjuna G., aged 49 years

Residing at 502, Bhaskara, TIFR Residential Complex,

Homi Bhabha Road, Colaba,

Mumbai 400005

Ph No: 9821550469

Email ramakumarr@gmail.com

PAN No: ACKPG0188 R

nagarjunag@gmail.com

5. Prof. R. Ramkumar, aged 37 years,

PAN No: AJWPR9886 N

Residing at B2/12, Reserve Bank of India,

Officer's Quarters, Chakala,

Andheri-East,

Mumbai 400 093

...Petitioners

Ph No: 9969109995

email no: ramakumarr@gmail.

4

Email nagarjun@gnnowledge.org

Versus

1. UNIQUE IDENTIFICATION AUTHORITY OF INDIA,

Planning Commission,

Government of India,

3rd Floor, Tower II,

Jeevan Bharati Building,

Connaught Circus,

New Delhi 110001

2. Mr. A. B. Pandey.

Deputy Director General, UIDAI,

Mumbai Regional Office,

5th & 7th Floor, MTNL Building,

BD Somani Marg, Cuffe Parade,

Mumbai 400 005

2. The Chairperson, Planning Commission of India,

Yojana Bhavan, Sansad Marg,

8 5
New Delhi.

3. National Informatics Centre

Department of Information Technology,
Ministry of Communications and Information Technology,
A-Block, CGO Complex,
Lodhi Road, ,New Delhi - 110 003 India

4. Union of India

Through the Ministry of Finance

New Delhi. 11 0 0 0 1

5. Union of India

Through the Ministry of Home Affairs

New Delhi. - 11 0 0 0 1

... RESPONDENTS

TO

THE HON'BLE CHIEF JUSTICE

AND THE OTHER HONOURABLE PUISNE

JUDGES OF THIS HON'BLE COURT

THE HUMBLE PETITION

8

OF THE PETITIONER
ABOVENAMED

MOST RESPECTFULLY SHOWETH:

PUBLIC INTEREST LITIGATION PETITION

1. Particulars of the cause/ order against which the Petition is made: The Petitioners are filing this public interest litigation to challenge the Notification dated 29th January 2009 that created the Unique Identity Authority of India (U.I.D.A.I.), an agency established under the aegis of the Planning Commission to issue Unique Identity Numbers (UID) to every Indian citizen.
2. The Petitioner submits that UIDAI was created through an executive fiat to enable the process of issuing UID cards across India, without any rules, procedures, or guidelines. Its further extension, universalisation and implementation across the nation remains must contingent upon both an initial success together alongwith legislative passage of the proposed National Identification Authority of India Bill, 2010 (hereinafter referred to as the NIDAI Bill). The Petitioners submit that in further developments by a report dated 13th December 2011, the Standing Committee of the Parliament has rejected the present draft of the NIDAI as not meeting the required constitutional standards.

- 7
3. However, in complete disregard to both, UID numbers without any safeguards against the tremendous breach of privacy entrenched in the scheme as it presently stands are being issued across the country without any legislative framework. Aside from this an ostensibly optional and a premature scheme is being converted into a mandatory requirement with the aid of different government agencies and state governments.

I. PARTICULARS OF THE PETITIONERS

1. Petitioner No. 1 is an engineer and manager by training. He is engaged with an ongoing project to understand issues around awareness of personal privacy rights across Asia. In the course of earlier globally recognised projects to develop specialised software for the profoundly disabled and communication solutions for poverty-stricken rural and urban dwellers, he has together with colleagues observed empirically that privacy concerns are palpable across different strata of society. The Petitioner submits that the present move to tag every Indian resident with unique numbers, a massive project of unknown scope and questionable possibility of success, is made increasingly dangerous as it may lead to access to personal information by third parties.

2. Petitioner No. 2 is a human rights activist with background in clinical psychology, journalism and law. She is an expert on gender, health and human rights and part of various networks and campaigns related to these issues. She has been active in 'Say No to UID' campaign which has disseminated much needed information about the UID in various forums including colleges, slums and NGOs in order to generate a much wider public discussion on the subject.

3. Petitioner No. 3 is a social work graduate from Tata Institute of Social Sciences. He has been a counsellor for two years and then crossed over into Journalism. For the past 15 years he has been a journalist with The Indian Express, rediff.com, NDTV and DNA. His forte has been reporting on issues of development and public interest. Since the launch of UID the Petitioner has been reporting on the issue through both news reports and columns against it and the regime it unleashes.

4. Petitioner No. 4 is one of the founding members of the FSF India and is currently serving as its Chairperson. He holds a faculty position at Homi Bhabha Centre for Science Education, TIFR in

9

Mumbai. He is an author and maintainer of the GNU project GNOWSYS, and leads the gnowledge.org lab in Mumbai. He holds an M.Sc.(Biology), M.A. (Philosophy) from the University of Delhi and a Ph.D. from the Indian Institute of Technology Kanpur in the area of Philosophy of Science. He advocates the appropriate use of technology and is opposed to the indiscriminate deployment of technologies in the UID project by UIDAI or its agents without a feasibility study or assessment of its risks.

5. Petitioner No 5 is an Associate Professor at the Tata Institute of Social Sciences, Mumbai. His official webpage is at <http://www.tiss.edu/faculty/Ramakumar>. He is an economist by training. He holds a PhD in Quantitative Economics from the Indian Statistical Institute, Kolkata and has worked and taught at the El Colegio de Mexico, Mexico City and the Centre for Development Studies, Trivandrum. His areas of interest are development economics, agricultural economics and rural development. He has published research papers and articles in many peer-reviewed international journals and books. He has been a close observer of the UID project from 2009 onwards and has written articles in **The Hindu** and **Frontline** on the subject. His research paper on the UID project titled "Unique ID Project in India: A

A

Skeptical Note" was published in 2010 by the international Springer journal, "Lecture Notes in Computer Science".

6. Respondent No. 1 is the impugned UIDAI authority which functions under an executive authority, through the impugned executive notification dated 28th January 2009. Respondent No. 2 is the regional UIDAI authority for the Mumbai Region, responsible for registering and enrollment for the UID scheme through the help of government agencies and private parties. Respondent No. 3 is the Planning Commission of India which has played a crucial role in conceiving the UID scheme and its current planning and implementation.

7. Respondents Nos. 4– 6 are different agencies and ministries that have independently expressed concerns about duplication, lack of safeguards, excessive expenditure with the present UID scheme before the Standing Committee of the Parliament. Quoting from the report of the Standing Committee:

"The Committee regret to observe that despite the presence of serious difference of opinion within the

*Government on the UID scheme as illustrated below,
the scheme continues to be implemented in an*

- i The Ministry of Finance (Department of Expenditure) have expressed concern that lack of coordination is leading to duplication of efforts and expenditure among at least six agencies collecting information (NPR, MGNREGS, BPL census, UIDAI, RSBY and Bank Smart Cards);*
- ii. The Ministry of Home Affairs are stated to have raised serious security concern over the efficacy of introducer system, involvement of private agencies in a large scale in the scheme which may become a threat to national security; uncertainties in the UIDAI's revenue model;*
- iii. The National Informatics Centre (NIC) have pointed out that the issues relating to privacy and security of UID data could be better handled by storing in a Government data centre;*
- iv. The Ministry of Planning have expressed reservation over the merits and functioning of the UIDAI; and the necessity of collection of iris image;*

28

- 12
- v. *Involvement of several nodal appraising agencies which may work at cross-purpose; and*
 - vi. *Several Government agencies are collecting biometric(s) information in the name of different schemes."*

All the Respondents are amenable to the Writ Jurisdiction of this Hon'ble Court.

II. DECLARATION AND UNDERTAKING OF PETITIONERS

1. That the present Petition is being filed in public interest. Petitioners No.1, 2, 3, 4 & 5 do not have any personal interest in the matter.
2. That the entire litigation costs, including the Advocates fees and other charges are being borne by the Petitioners.
3. That a thorough search has been conducted in the matter raised through the Petition and all the material concerning the same has been annexed to this Petition.
4. That to the best of the Petitioners knowledge and research the issue raised was not dealt with or decided and a similar or identical petition was not filed earlier by the Petitioners.
5. That the Petitioners have understood that in the course of hearing of this Petition the Court may require any security to be

&

furnished towards costs or any other charges and the Petitioners shall have to comply with such requirements.

6. In the absence of parliamentary approval, and in the light of the scathing review of the performance of the UIDAI by the Parliamentary Standing Committee on Finance, citizens are left with no alternative but to approach the Hon'ble Court to place an embargo on *Aadhaar*, until it undergoes full Parliamentary scrutiny to evaluate its effectiveness and Constitutionality.

7. The Petitioners submit that through this PIL they represent a much wider discontent with the UID scheme that has been expressed in numerous foras. A recent letter by prominent writers, lawyers, historians, and judges has argued strongly for constitutional safe guards in UID. To reproduce the content of the letter below:

"A project that proposes to give every resident a "unique identity number" is a matter of great concern for those working on issues of food security, NREGA, migration, technology, decentralisation, constitutionalism, civil liberties and human rights. The process of setting up the Unique Identification Authority of India (UIDAI) has resulted in very little, if any, discussion about this project and its effects and fallout. It is intended

(S)

14
to collect demographic data about all residents in the country.

Before it goes any further, we consider it imperative that the following be done:

(i) Do a feasibility study: There are claims made in relation to the project, about what it can do for the PDS and NREGA, for instance, which does not reflect any understanding of the situation on the ground. The project documents do not say what other effects the project may have, including its potential to be intrusive and violative of privacy, who may handle the data.

(ii) Do a cost-benefit analysis: It is reported that the UIDAI estimates the project will cost Rs. 45,000 Crores to the exchequer in the next four years. This does not seem to include the costs that will be incurred by the registrars, enrollers, the internal systems costs that the PDs system

3

will have to budget if it is to be able to use the UID, the estimated cost to the end user and to the number holder.

(iii) In a system such as this, a mere statement that the UIDAI will deal with the security of the data is obviously insufficient. How does the UIDAI propose to deal with data theft?

(iv) The involvement of firms such as Ernst & Young and Accenture PLC raises further questions about who will have access to the data, and what that means to the people of India. The questions have been raised which have not been addressed so far, including those about:

- (i) Privacy: It is only now that the Department of Personnel and Training is said to be working on a draft of a privacy law, but nothing is out for discussion,
- (ii) Surveillance: This technology, and the existence of the UID number, and its working, could result in increasing

the potential for surveillance,

(iii) *Profiling,*

(iv) *Tracking, and*

(v) *Convergence, by which those with access to state power, as well as companies, could collate information about each individual with the help of the UID number. National IDs have been abandoned in the US, Australia and the UK. The reasons have predominantly been costs and privacy. If it is too expensive for the US with a population of 308 million, and the UK with 61 million people, and Australia with 21 million people, it is being asked why India thinks it can prioritise its spending in this direction. In the UK the home secretary explained that they were abandoning the project because it would otherwise be "intrusive bullying" by the State, and that the government intended to be the "servant" of the people, and not their "master". Is there a lesson in it for us?*

17

This is a project that could change the status of the people in this country, with effects on our security and constitutional rights. So a consideration of all aspects of the project should be undertaken with this in mind.

We, therefore, ask that the project be halted; a feasibility study be done covering all aspects of this issue; experts be tasked with studying its constitutionality; the law on privacy be urgently worked on (this will affect matters way beyond the UID project); a cost-benefit analysis be done; a public, informed debate be conducted before any such major change be brought in.

Justice V R Krishna Iyer,

Romila Thapar,

K G Kannabiran,

S R Sankaran,

Upendra Baxi,

Shohini Ghosh,

Bezwada Wilson,

Trilochan Sastry,

Jagdeep Chhokar,

Justice A P Shah,

and others."

8

Eth-A'

Till date there is no response from the Respondents to numerous such representations. Copy of the aforesaid letter is annexed hereto and marked as Exhibit A.

III. ISSUES:

- i. The rejection of the UID Scheme as represented through the NIDAI Bill by the Standing Committee of the Parliament, calls for an immediate cessation of the executive scheme of UID.
- ii. Aadhaar/UIDscheme needs to be quashed for breach of Articles 14, 15, 19 and 21 of the Indian Constitution.
- iii. The *Aadhaar* numbers scheme as it stands is unconstitutional as it vests in the State immense power to monitor the activities of Indian residents and violate their fundamental right to privacy.
- iv. There is no rational nexus between the collation and convergence of personal data of every citizen and the stated objective of UID, which is primarily to improve the distribution of welfare services.
- v. Given that biometrics cannot succeed in creating a unique identification, the objective of non-duplication cannot rationally be achieved by invasive means of collecting personal information, which is a grave beach of the right to privacy. Any subsequent tampering of the biometric information contained in

the proposed database of personal information will result in unprecedented damage to the right to life and liberty of the affected person or persons.

vi. The technology adopted by UIDAI for the capture of biometric information ie digital fingerprint recording, is known to be insufficiently accurate to function as an identifier. An additional biometric identifier, iris scanning, has been found to be too expensive to be universally deployed. Thus the use of biometric identification to uniquely authenticate and verify the identities persons residing in India, upwards of 130 crore persons at the time of filing this petition, is unsuitable, leaving UIDAI's proposed solution to the problem of issuing persons in India unique identity numbers infructuous and necessitating cessation of this risky, invasive and expensive project.

vii. Collection of data by outsourcing enrolment for *Aadhaar* has huge implications on privacy

viii. Convergence and collation of personal information in a digital form and unrestricted access to such information by the National Intelligence Grid, without any legislated and constitutional safe guards is a grave breach of the right to privacy enshrined in Article 21 of the Constitution.

ix. Should the Courts not intervene to put an embargo on *Aadhaar*, until it undergoes parliamentary scrutiny to evaluate its effectiveness and constitutionality?

- 20
- x. The non-mandatory nature of implementation of Aadhaar, through excessive delegation of powers to sub-registrars under the scheme has both gone beyond the voluntary nature of the scheme, and created greater potential for leakage and misuse of sensitive personal information; without any legislative safeguards.

IV. FACTS IN BRIEF CONSTITUTING THE CASE.

1. The Unique Identity Project (the "UID"), a brainchild of the Planning Commission, was announced with the ambitious agenda of collecting and documenting biometric and other information of the entire Indian population. To this end, the Planning Commission also set up an independent authority, through an executive order of the Central Government, with the mandate of implementing the UID. UID aims at becoming the primary basis for efficient delivery of welfare schemes by converting itself into a statutory corporate body which would go by the name of the National Identification Authority (the "Authority").
 2. Unique Identity Number is in addition to other identities and is issued to all the citizens from time to time like PAN Card, Passport, Ration Card, Driving License, BPL Cards, NREGA Card and similar cards issued by both State and Central Government. However, unlike these need based identities
- 3

issued by the government to various citizens of India, the UID number is issued to every resident in India. It is stated that the said identity number is an option that a resident can choose to take as it would be easy to authenticate a person's identity anywhere and thus is portable. The identity will be stored in a central database with individuals biometric and demographic data linked to a randomly generated unique number. The identity would be authenticated by querying the database. Thus, it may be seen that even a person possessing the UID or AADHAAR card cannot authenticate his or her identity, but only those in charge of the UID database have the means and authority to authenticate the person's identity. The 12 digit number would be assigned as UID to every resident would be integrated with biometric and demographic data of the person. Demographic data here means the details of the person that is his name, name of the father (only in case of a child below the age of five years), age, residential address, telephone number, email address, details of bank accounts. Biometric data is collection of digitized images of all the fingerprints and scanning of irises and image of the face. A copy of the application form is annexed hereto and marked as Exhibit B. Copy of the UID Strategy Overview dated April 2010 issued by Respondent No. 1 is annexed hereto and marked as Exhibit C. Copy of a detailed alternative note that critically explains the functioning of the

Exh-BExh-C

22

UID titled "UID for Dummies" authored by Simi Chacko and Pratiksha Khanduri dated 12th September 2011, is attached hereto and marked as Exhibit D.

Exh-C-1

3. The Petitioners submit that the twin proposals to create both a National Population Register by an amendment to the Citizenship Rules and UID, were brought into the purview of an empowered group of Ministers (EGoM) constituted on 4th December 2006.

4. Initially the UIDAI may be notified as an executive authority and investing it with statutory authority could be taken up for consideration later at an appropriate time.

I. UIDAI may limit its activities to creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.

II. UIDAI will take its own decision as to how to build the database.

III. UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.

A

IV. Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure through the DoE/CCEA.

V. Approval to the constitution of the State UIDAI Authorities simultaneously with the Central UIDAI with a core team of 3 personnel.

VI. December 2009 was given as the target date for UIDAI to be made available for usage by an initial set of authorized users.

VII. Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed organizational structure, staff and other requirements.

background to the UID
Copy of the ~~recommendations dated 04 November 2008~~ is

annexed hereto and marked as Exhibit E.

Exh-E

5. In pursuance of the recommendations of the Committee of Secretaries and the Empowered group of Ministers' the Unique Identification Authority of India was constituted and

24

notified by the Planning Commission on 28 January 2009 as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. The role and responsibilities of the UIDAI was laid down in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UIDAI scheme and own and operate the UIDAI database and be responsible for its updation and maintenance on an ongoing basis. Copy of the Notification dated 28th January 2009 is annexed hereto and marked as **Exhibit F**. The said impugned Notification outlined the following tasks to be carried out under the UID banner:

P. 186
Exh-F

- I. Generate and assign UID to residents
- II. Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
- III. Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
- IV. Co-ordinate/liase with implementation partners and user agencies as also define conflict resolution mechanisms
- V. Define usage and applicability of UID for delivery of various services
- VI. Operate and manage all stages of UID lifecycle

4

- VII. Adopt phased approach for implementation of UID specially with reference to approved timelines
- VIII. Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- IX. Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
- X. Evolve strategy for awareness and communication of UID and its usage
- XI. Identify new partner/user agencies

6 The Petitioner submits that subsequent to the notification the Government appointed Shri. Nandan M. Nilekani as Chairman of the Unique Identification Authority of India, in the rank and status of a Cabinet Minister for an initial tenure of five years. Mr. Nilekani has joined the UIDAI as its Chairman on 23 July 2009. Copy of the notification appointing Nandan M. Nilekani as chairman is annexed hereto and marked as Exhibit G.

P-123
11/11/09Exh- G.

7 The Petitioner submits that although set up through an executive fiat, the UIDAI was always intended to be brought under the purview of a legislative scheme. In the meanwhile, an advisory council presided by the Prime Minister's was set

up on 30 July 2009. The Council is to advise the UIDAI on Programme, methodology and implementation to ensure co-ordination between Ministries/Departments, stakeholders and partners. Further, the activities of the UIDAI were to be supervised and monitored by a Cabinet Committee headed by the Honourable Prime Minister and consists of the Minister of Finance, Minister of Agriculture, Minister of Consumer Affairs, Food and Public Distribution, Minister of Home Affairs, Minister of External Affairs, Minister of Law and Justice, Minister of Communications and Information Technology, Minister of Labour and Employment, Minister of Human Resource Development, Minister of Rural Development and Panchayati Raj, Minister of Housing and Urban Poverty Alleviation and Minister of Tourism. The Deputy Chairman Planning Commission and Chairman UIDAI are special invitees.

8. Thus it is clear that in its present form UIDAI is an executive body with no legislative authority intended at this juncture to create the systems for the long term universal implementation of UIDs pursuant to the enactment of a legislative scheme and an appropriate regulatory authority. The Petitioners submit that before the legislative scheme is enacted, the Parliament as a sovereign body, will scrutinize the "suspect" claims made by UID and the effectiveness, feasibility and

constitutionality of its objectives. The Petitioners submit that the constitutionality of the UID as an executive scheme without any legislative backing is further suspect pursuant to the rejection of the NIDAI Draft Bill by the Standing Committee of the Parliament, for falling short of meeting minimum constitutional standards.

9. The Petitioners submit that the eventual aim of the *aadhaar* numbers scheme is to streamline the delivery of services to Indian residents and avoid corruption and misuse of public funds and subsidies. UIDAI claims that the UID will achieve the two following objectives:

- a. Revolution in public service delivery. By providing a clear proof of identity, Aadhaar will empower poor and underprivileged residents in accessing services such as the formal banking system and give them the opportunity to easily avail various other services provided by the Government and the private sector. The centralised technology infrastructure of the UIDAI will enable 'anytime, anywhere, anyhow' authentication. Existing identity databases in India are fraught with problems of fraud and duplicate or ghost beneficiaries. To prevent these problems from seeping into the Aadhaar database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric

information. This will ensure that the data collected is clean from the beginning of the program. However, much of the poor and under-privileged population lack identity documents and Aadhaar may be the first form of identification they will have access to.

- b. Overhaul internal security and assist the investigating agencies.

10. To achieve its objective as stated above, UID has set out to undertake its main task that is of Data Collection, without the legislative passage of the NID Bill. The Petitioner submits that the creation of a national identity card or number requires the following activities:

- i. DATA COLLECTION: Information relating to the individual necessary for identification is collected and stored in a register under the supervision of a governmental authority. This may include different categories of sensitive, personal information about individuals from their health records, to bank transactions, to the number of times they may use public transport every week.
- ii. DATA PROCESSING: The Authority either discloses or verifies the information in the register upon any requests regarding any individual permitted under any law; and

iii. DATA PROTECTION: The government is duty bound to protect such information.

iv. DATA DESTRUCTION: The government is duty bound to destroy such sensitive, personal information as is not absolutely needed for the functioning of a scheme of authentication of identity cards or numbers, and has been collected for that purpose, and should not be retained or used for any other purpose without the full informed consent of each and every enrollee.

11. The main function of the Authority is to collect relevant personal details together with unique biometric information from the population and use this information as the basis for issuing unique identification numbers to the population. The unique numbers, which are referred to as *aadhaar* numbers, are to be used as the basis of authentication of the identity of Indian residents seeking to avail certain services, either from the State or private parties. While authenticating the identity of a user, the proposed Authority only confirms or denies the authenticity of the number and its holder, i.e., by way of a simple 'Yes' or 'No' answer. The UIDAI has stated that the proposed authority does not propose to disclose, to a third party, any of the personal details it may have collected in order to issue the *aadhaar* number. However, the Authority

in a central database will store details of all authentication requests received for a particular *aadhaar* number. On analyzing these authentication requests it is possible to track the location and utilization of services by the holder of an *aadhaar* number. This can create immense potential for misuse of information, leaking of personal information in the wrong hands. Apart from this, UID, in an open premise has committed itself to sharing all information collected by it with the National Intelligence Grid. Copy of a detailed scientific study by Paul Ohm titled "Broken Promises of Privacy: Responding to the surprising failure of Anonymisation" that illustrates how central identity databases facilitate the reverse audit trail of personal information is attached hereto and marked as Exhibit H.

Exh-H

12. The UIDAI has conducted a so-called 'proof of concept' study that determined the expected rate of failure of biometric measurement as an identification method. The report is attached hereto and marked Exhibit I. An analysis of the reported figures reveals that the conclusions drawn in this report are insufficiently precise, and in fact, the incidence of so-called 'false positives' (persons incorrectly identified by the measuring system) will be impossibly high. A copy of this analysis by David Moss, a British engineer responsible

Exh-I

31

for similar studies that showed the impossibility of the now-cancelled (at a loss of substantially over stg 800 million, approximating Rs 6,500 crores) UK ID cards system is attached as Exhibit J.

Exh - J

13. The draft NIDAI Bill lays out a regulatory framework identifying the powers and responsibilities of the proposed Authority along with criminal sanctions for unauthorized disclosure of information collected by the Authority. However, the same are highly inadequate and fail to meet the minimum standards of safeguards necessary. In a legal atmosphere with no legislated right to privacy, the enforcement of weak criminal sanctions against any breach of privacy becomes difficult. Copy of the UIDAI Bill is annexed hereto and marked as Exhibit K. Copy of an article titled "A Unique Identity Bill" by Prof. Usha Ramanathan, a prominent advocate on the right to privacy in India, is annexed hereto and marked as Exhibit L.

Exh - K

Exh - L

14. The Petitioners submit that the UIDAI draft as it was tabled in the Parliament has been rejected by the Standing Committee by its report dated 13th December 2011, by the making the following observations:

a. Lack of clarity

b. Overlap between UID and NPR

15

- c. No statutory power to address key issues of defaulters and penalties
- d. Aadhaar will not completely eradicate the need to provide other documents for identification
- e. Estimated failure of biometrics is expected to be as high as 15% due to a large chunk of population being dependent on manual labour.
- f. It is also not clear that the UID scheme would continue beyond the coverage of 200 million of the total population, the mandate given to the UIDAI.
- g. Considering the huge database size and possibility of misuse of information has not been carefully considered.

Copy of the detailed report of the Standing Committee dated 13th

Exh-M December 2011 is annexed hereto and marked as Exhibit M.

V. RIGHT TO PRIVACY

15. The Petitioner submits that the proposal of data collection, storage and sharing as laid out above makes heavy inroads into the right to privacy and its constitutionality must be tested against the breach of the right of privacy itself enshrined under Article 21 and also for rationality and non-arbitrariness by examining the objective behind UID. The Petitioner submits that UIDAI attempts to undertake the task of collecting personal information for the entire Indian population, which constitutes a total of 1.2 billion people. The privacy implications of the same are numerous and as follows:

I. Data Collection:

- i. **Sub Registrar:** UIDAI in order to expedite the collection of information has entered into MoUs with several agencies, be it Banks, Insurance Agents, other Government Departments to enroll citizens for the UID card. Even though UIDAI, only allows for collection of non-sensitive personal information, through the decentralization and delegation of data collection, the Sub-Registrar has been provided with the freedom to ask for additional information. Thus, for example, every Aadhaar form has the option of linking your bank

34

account with the Aadhaar number. The Petitioners submit that in many reported cases, the Banks acting as Sub-registrars, automatically link the bank accounts with the Aadhaar while registering new entrants. Some of the excessive information sought from sub-registrars includes:

1. Resident's name, his/her father's name, his/her spouse's name, names of his/her children, his/her age, residential address, his/her income, whether he/she owns any car? Whether he/she owns any scooter? Whether he/she owns any other vehicle? His/her telephone and cell phone numbers both office and residence, his/her deposits, insurance policies, investments, the companies in which he/she has interest and other details;

2. Similar details regarding spouse and children, linked with the Aadhaar number are collected. All these details are not collected under the Aadhaar form. However, all these particulars are mandated through the concept of 'Know Your Customer' from the banks by a RBI directive. When all these details of each resident is integrated, the

A

state would be virtually accessing and intruding into the life of each and every resident of India, through Dr. Usha Ramanathan's argument on convergence of different silos of information.

- ii. **Excessive Delegation:** By appointing several sub-registrars and empowering them with data collection and registration, sensitive personal information about citizens instead of going directly to the UIDAI data base also becomes available in a parallel format with the Sub-Registrar, who is not bound by ~~any rules, regulations or legislative framework~~ to protect. Copy of recent news report of theft and sale of enrolment data from private agencies in Punjab is annexed hereto and marked as **Exhibit N.**

Exh- N

16. **Data Storage in One Central Database:** It further contemplates storage of that entire information in one central data base. The Respondents also claim that it will be safe. It is submitted that biometric and demographic information of 1.3+ billion residents of India mean 6 petabytes (6,000 terabytes or 6,000,000 gigabytes). It will be the world's largest database. The technological challenges are enormous and involve system performance, reliability,

speed and resolution of accuracy and errors. But a more serious issue is regarding the security. The information can be hacked. The Petitioners respectfully submit that hacking of data is not a theoretical fear, but a practical reality. The implications of this cannot be settled just through a Proof of Concept.

I. Data Protection

- i. **Audit Trail:** According to UIDAI, when you enter into a transaction where you had to produce your ID card, the design of the system was such that a record would be kept of every such verification. It provides a detailed record of every transaction done, which can be of interest to either people browsing the database or to security services or whoever. UIDAI, argues that the record here is limited to verification and thus even if traced back to the source of service accessed, it remains harmless. However, the record here would not be just the verification of identity; there would be a little more data associated with the transaction. In a recent published interview, a scholar working on the conflict between privacy and National ID cards, cites the following apposite example:

"For example, you went to Health Clinic Number 45. They used your card and your fingerprint there for verification. They did this at 12:37 hours. There is a series of metadata associated with that visit that would be there in the audit trail. And, of course, it wouldn't take very long to realise that, actually, Health Clinic Number 45 is a sexual health clinic. If the audit trail also shows that you were there on a number of occasions, it might be reasonable to infer certain kinds of things that you perhaps do not want to disclose. Some things are not necessary to be disclosed, but which are being recorded and stored in an accessible way to various people because of the way the system is designed." A copy of the Edgar Whitley interview printed in Frontline is annexed hereto and marked as Exhibit O. *Exh O.*

- ii. **Disclosure of Information:** The potential of audit trail misuse is an important reality. In the present form UIDAI has no mechanisms for preventing the sharing of any information, or safeguards/penalties for leaks and misuse of verification records. The NID Bill, however

contemplates misuse and hence provides the following framework:

- a. Cl. 33 "Nothing contained in the sub-section (3) of section 30 shall apply in respect of – (a) any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or (b) any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer not below the rank of Joint Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge."

Clause 33, is highly inadequate, as firstly it excludes information sought for nsecurity reasons from judicial scrutiny. This in itself is a recipe for grave misuse of private information. On the other hand court orders are not subject to the rule of *audi alteram partem*.

4. **Destruction of Data:** The UIDAI has described its operational method for authentication of enrollees as

requiring the person to present the number and biometric information (initially, fingerprints, up to ten; however it has been asserted from time to time that only two fingerprints will be necessary for authentication; in the absence of any trials of the system, such fine details are not known at present. The need for iris scans has also been expressed, however, the budget for recording iris scans has not been approved, nor have the present numbers of the population, said to be over 10 cr, had iris scans taken at the time of enrolling with UIDAI). The information will be matched with the information in UIDAI's central database and a simple yes/no reply will be generated. No personal details of any kind can be sought from the database through this system. It is obvious that other personal details are only taken for the purpose of verifying the accuracy of the basic information ie matching the fingerprints with the person. It is not needed for the further functioning of the system, as claimed by UIDAI. It is therefore essential that the additional data collected be destroyed in order to protect citizens from any illegal access to the UIDAI database and subsequent misuse of that breach of privacy in any way whatsoever. UIDAI has not made any provisions at all for data destruction, although it is well known in technological circles that destruction of digital data is an expensive and tedious task.

40

17. It is important to note that the Right to Privacy especially in the context of wrongful access to personal information about individuals and controlling excessive interference from the State into private lives of individuals, is well recognized in Indian law. It has been held that the Right to Privacy is an integral part of the Right to Life under Article 21.

18. In *Kharak Singh v. State of Uttar Pradesh*¹, a person with a criminal record, had challenged the constitutionality of certain police regulations which permitted surveillance of his house as also 'domiciliary visits' to his house at any time. In this case the petitioner had attempted to put forth the argument that the regulations in question violated his right to privacy which could be read into the fundamental right to life and liberty in Article 21 of the Constitution. The majority judgment of the Court however rejected this argument that Article 21 of the Constitution provided for a fundamental right to privacy. The minority judgment by Justice Subba Rao and Justice Shah however favoured a broader interpretation of the term 'personal liberty' in Article 21. In pertinent part, Justice Rao held that "*It is true our Constitution does not expressly declare a right to privacy as a fundamental right,*

but the said right is an essential ingredient of personal liberty"

19. The debate over 'privacy as a fundamental right' cropped up once again in the case of *Gobind v. State of Madhya Pradesh*. The petitioner in this case had challenged certain police regulations on the grounds that the same had invaded the petitioner's fundamental right to privacy. In this judgment a full bench of the Supreme Court was more willing to link the 'right to privacy' to the fundamental rights enshrined in Part III of the Constitution. The Court has held that the Right to Privacy clearly means one has a right to be left alone within one's home.

"Rights and freedoms of citizens are set forth in the Constitution in order' to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. 'Liberty against government' a phrase coined by Professor Corwin expresses this idea forcefully. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy."

Y

42

20. The aforesaid quote is pertinent in understanding the kind of unfettered intrusion access UIDAI and the NID Bill allow into the State and many other private agencies into the personal lives of citizens of India, without any legislative procedures, safeguards and remedy. Thereafter, the right to privacy has been recognized in a number of judgments of this Court and of the High Courts in a number of cases including *PUCL v. Union of India* (1997) 1 SCC 301, *Sharda v. Dharampal* (2003) 4 SCC 493, *R. Rajgopal v. State of Tamil Nadu* (1994) 6 SCC 632, *Phoolan Devi v. Shekhar Kapur* (57 (1995) DLT 154), *Khushwant Singh v. Maneka Gandhi* AIR 2002 Del 58.

21. And more appositely, in the case of *District Registrar and Collector, Hyderabad v. Canara Bank* (2005) 1 SCC 632, section 73 of the Andhra Pradesh Stamp Act was challenged. The impugned section required any public officer or any other person having in his custody records, registers, books, documents, the inspection of which may result in discovery of fraud or omission of duty, to allow any person authorized in writing by the collector to enter any premises to conduct an inspection of the same which may also be impounded by the person so authorized after due acknowledgement of the same.

23

22. This provision was struck down by the High Court of Andhra Pradesh on the grounds that it was arbitrary and unreasonable and the same was upheld by the Supreme Court. In arriving at its conclusions the Court held that legislative intrusions into a person's privacy "must be tested on the touchstone of reasonableness as guaranteed by the Constitution and for that purpose the Court can go into the proportionality of the intrusion vis-à-vis the purpose sought to be achieved." In a later portion of the judgment the Court while harshly criticizing the lack of any procedural safeguards or mechanism in the impugned provision went on to cite its own precedent in the case of "Air India v. Nergesh Meerza & Ors., (1981) 4 SCC 335, where "it was held that a discretionary power may not necessarily be a discriminatory power but where a statute confers a power on an authority to decide matters of moment without laying down any guidelines or principles or norms, the power has to be struck down as being violative of Article 14."

VI. RATIONAL NEXUS BETWEEN UID AND THE POLICY OBJECTIVE\

23. The Petitioners submit that the UIDAI has made statements in public that through a study titled, 'PROOF OF CONCEPT' they have developed a fool proof method and with minimal error margin. The Petitioners submit that the purpose of any

44

feasibility study must be to conclusively establish that the objectives sought to be achieved will be accomplished through the exercise, especially when a vast amount of public money is at stake.

24. Thus, in the case of the UID project, where the objectives, according to the statements of the Respondents, are to ensure welfare benefits reach the intended beneficiaries, it would be necessary for the PoC exercise to show how beneficiaries would receive these benefits. This means, that the study would involve, not merely the collection of fingerprint data, but the use of the data to authenticate the BPL beneficiaries who come to collect PDS rations from designated shops and their receiving the goods over a reasonable period of time through the process envisaged in the project. Thus in a nutshell a feasibility study should not be a theoretical, imaginative exercise like the POC, but something that is tested in practice over a period of time.

25. The Petitioner submits that the primary purpose of UIDAI is said to be to improve the welfare system in the country by eradicating identity theft through duplication of identity. Thus non-duplication has been championed as both the solution for fixing the old Public Distribution System, and UID as the "unique" method of achieving it.

\$

26. The Petitioners submit the foremost assumption in the aforesaid is that due to lack of identity the poor do not receive government welfare benefits. Secondly, the Respondents assume that fake and duplicate identities are the causes for leakage (that is siphoning) of welfare funds. Both these are unproven assumptions. They are not based on any study or investigation. Several studies have increasingly shown that the PDS system is actually improving, and that by introducing an untested new Aadhaar, universally and across the board in a rushed manner, may actually end up excluding a lot of intended beneficiaries. Copies of detailed reports, analysis and studies conducted on the efficacy of UIDAI to address welfare distribution issues conducted and written by Prof. Reetika Khera are annexed hereto and marked collectively as Exhibit P.

Exh-P'

27. UIDAI argues that through the combination of name, photograph, fingerprinting and iris scans they can create an irrefutable identity that is linked to the person itself, and does not require any external proof – like ration cards or passports for identification. The person herself is the identifier through fingerprinting and iris scans.

1

46
28. However, there are many problems with this proposition.

Firstly, a data base of this scale of 1.2 billion people's finger prints and iris scans has never been created. Thus the entire proposition for a population base such as India is completely untested and unproven. Quoting an analogy that criticizes the similar UK ID Cards' non-duplication strategy which was entirely scrapped:

There were far better performance results on a 1:1 match. So, this is Edgar's fingerprint on the database, here is Edgar, we do 1:1 match; this is more likely to work. But that was not how the U.K. was planning to use it. The U.K. was trying to use biometrics to also prevent duplicate identities. The idea was that even if I try to enrol twice, and even if I had created a fake biographic identity (say, a John Smith with a different address), when my fingerprint came in for a second time, the system should come along and say: "We know this fingerprint, and this belongs to Edgar Whitley" and not say, John Smith. Here, you have to match every single biometric with every single previous biometric."

29. Thus biometrics requires not just matching a fingerprint with its true origin, but also with others to avoid non-duplication.

§

47 47

Apart from this exercise, the very reliability of finger prints in India is not 100 percent. An assessment report filed by 4G Solutions, contracted by UIDAI to supply biometric devices, notes:

"It is estimated that approximately five per cent of any population has unreadable fingerprints, either due to scars or aging or illegible prints. In the Indian environment, experience has shown that the failure to enrol is as high as 15 per cent due to the prevalence of a huge population dependent on manual labour."

Copy of the 4G Solutions Report is annexed hereto and marked as Exhibit Q.

Exh Q.

30. The report of the UIDAI's "Biometrics Standards Committee" actually accepts these concerns as real. Its report, notes that "fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context." Thus, the very premise of UIDAI is not something that has scientific backing. This consideration has formed an important basis behind the decision of the Standing Committee rejecting the UIDIA bill and scheme as it presently stands. Copy of the Biometrics Standards Committee report commissioned by the UIDAI is annexed hereto and marked as Exhibit R.

Exh-R.

48

VII. Mandatory and Coercive

31. The Petitioners submit that one of the biggest illegalities being committed under the Aadhaar scheme is by making it mandatory through coercive conditions. UID has always, repeatedly stated that Aadhaar is a voluntary scheme. Thus, enrolment for Aadhaar is a voluntary act. The NIAI draft Bill, which seeks to legitimize the functioning of the first Respondent, is so worded to establish that Aadhaar is optional and not compulsory. However, in its premature implementation, in practice the scheme is gradually being made non-voluntary and mandatory. This is made worse by adoption of coercive pre-conditions by different government departments.

i. A recent gazette notification dated 26 Sep 2011, of the Petroleum Ministry has made Aadhaar a mandatory condition for LPG users. Copy of the news report announcing the change in policy is annexed hereto and marked as Exhibit 'S'

ii. Government of Maharashtra through its GR dated April 2011, plans to make Aadhaar a compulsory requirement for government employees for accessing their salary benefits. Copy of the aforesaid circular is annexed hereto and marked as Exhibit 'T'

8

32. The Petitioners submit that the enrollment for Aadhaar is working on an extremely fast pace that it has become impossible to avoid attempts at enrolment. The Petitioners submit that such mandatory, non-voluntary and coercive enrolment for Aadhaar is an affront to their to personal integrity, right to make decisions about themselves and the right to dignity all enshrined and developed as indivisible elements of the Right to Life under Article 21 of the Constitution.

33. The Petitioners submit that by insisting on a mandatory requirement and making access to every service contingent upon Aadhaar, the Respondents are creating a class of excluded non-Aadhaar holders who will be left out of welfare schemes, because they have consciously chosen to not enroll in an untested, premature and at present completely unreliable scheme.

34. The Petitioners submit that Aadhaar must be enacted not only under the supervision and protection of a strict national privacy law, but even in its implementation it must only be brought in through a phased manner, and not the sudden immediate implementation as at present.

GROUNDS

§

50

- A. The UIDAI-Aadhaar scheme as it presently stands as a mere executive fiat, is illegal, arbitrary and unconstitutional by granting wide, unrestricted powers to an unaccountable independent body known as UIDAI, and also to private agencies; leading to huge breaches on the right to privacy and dignity of Indian citizens;
- B. Reasonable restrictions on fundamental rights can only be through legislative mandate. The UID scheme makes invasion into fundamental rights without a legislative mandate and is hence bad in law;
- C. The co-extensive executive power exercised to implement UIDAI cannot be untrammelled and function towards restricting fundamental rights without any due procedure, guidelines and safety mechanism, which can only be ensured through a statutory framework;
- D. The Hon'ble Supreme Court has repeatedly held that executive power cannot be used to restrict fundamental rights;
- E. The mandatory enforcement UIDAI-Aadhaar scheme contravenes Article 21 by restricting the right to decision making, personal integrity, choice and dignity;
- F. The impugned notification dated 4th November 2008 is illegal, arbitrary and bad in law for setting out an extensive task of launching UID way beyond the executive competence, without any guidelines, rules and procedure;

§

- 52 57
- G. The aforesaid impugned notification is illegal, arbitrary and unconstitutional and in breach and contravention of Article 14 for assigning the most essential function of data collection via enrollment for Aadhaar to private agencies;
- H. The aforesaid notification is further illegal as it delegates excessive powers with the UIDAI without any guidelines or procedure, leading to further unrestricted delegation of powers to private parties creating great potential for data leakages, and breaches of sensitive private data leading to Indian Citizens;
- I. Cross-referencing service usage of a particular individual through a single numeric bio-metric identity has huge implications for building State inroads into every private activity and service accessed by that individual, this is further complicated by the possibility of private actors also accessing similar information. This convergence of silos of information will completely abolish the veneer of privacy that protects the daily lives of individuals.
- J. The Hon'ble Supreme Court of India has repeatedly upheld the right to privacy within the right to life in Article 21, and any restriction must be justified through a rational and reasonable statutory procedure. UIDAI, as it presently stands is prima facie unconstitutional for contravening the right to privacy without providing any safeguards, procedures and guidelines
- K. The UIDAI is further frought and arbitrary for failing to provide a rational nexus between means adopted of obtaining sensitive

52

personal information in a central database through private, or public-private partnerships for verification purposes in a central database and the ultimate objective of improving public welfare; wherein the whole premise is based on non-duplication of identity through biometrics, which still remains unproven.

L. The aforesaid impugned scheme is further in breach of right to dignity and personal autonomy enshrined under Article 21, by making the Aadhaar mandatory, thereby forcing people to submit themselves to an unreliable, untested, premature scheme which has no statutory standing and compromises their personal lives.

35. The Petitioners submit that they have not filed any other petition in respect of the present issue before this Hon'ble Court or the Supreme Court of India.

36. The Petitioners are residing at Mumbai Respondents are registered offices in Mumbai and New Delhi therefore the cause of action has arisen within the original side jurisdiction of this Hon'ble Court, hence, it can admit the petition and hear it.

37. The Petitioners state that they have no other alternative efficacious remedy but to approach this Hon'ble Court and the relief as prayed for if granted shall be complete.

38. The Petitioners will rely on documents a list whereof is annexed hereto.

39. There is no delay or laches in filing this petition.

A

40. The Petitioners have affixed the required court fees ____ to this Petition.

41. No caveat with regard to the subject matter of this petition has been received by the Petitioners till date.

PRAYERS PRAYED FOR:
THE PETITIONERS THEREFORE PRAYS

A. For a Writ of Certiorari or any writ, order, direction in the nature of certiorari or any other appropriate writ, order of direction quashing the notification dated 29th January 2008 annexed at Exhibit F;

B. For a writ of Prohibition or a writ, order or direction in the nature of prohibition or any other appropriate write, order of direction restraining the Respondents from taking any further steps of any nature whatsoever in relation to UID;

C. Till the final hearing and pendency of this Public Interest Litigation, this Hon'ble Court may be pleased to stay the operation of the impugned dated 29th January 2008 annexed at Exhibit F;

D. Till the final hearing and pendency of this Public Interest Litigation, this Hon'ble Court may be pleased to restrain the Respondents from taking any further steps of any nature whatsoever in relation to UID;

INTERIM ORDERS PRAYED FOR

E. For ad interim relief in terms of prayers C and D;

F. For any other orders that this Hon'ble Court may deem fit;

§

[Handwritten signature]

CAVEAT:

No Notice has been received of lodging a
 caveat by the opposite parties.

~~E. For ad-interim relief in terms of prayers C and D;~~

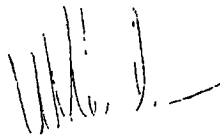
~~F. For any other orders that this Hon'ble Court may deem fit;~~

Petition drawn by me

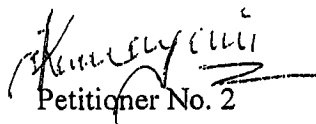


Mihir Desai

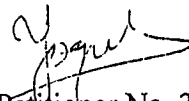
Advocate for the Petitioners



Petitioner No.1

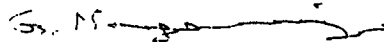


Petitioner No. 2



Petitioner No. 3

~~Petitioner No. 4~~



Petitioner No. 4



Petitioner No. 5

55

VERIFICATION

I, VICKRAM CHANDRA, as per the Petitioner No. 1
abovenamed residing at presently at Mumbai

do hereby state and solemnly declare that what is stated in paras No.

1 to 34 is true to my own knowledge and whatever is
stated in remaining paras no. 35 to para 41 is stated on information and
belief which I believe the same to be true.

Solemnly declared at Mumbai

On this 16th day of January 2012

} [Signature]
} Petitioner No. 1

Identified by me

[Signature]

MIHIR DESAI

Advocate for the Petitioners

Before me

[Signature]
16/01/2012
D. G. B. RAM
[Stamp]

16-1-12

**IN THE HIGH COURT OF JUDICATURE AT BOMBAY
ORDINARY ORIGINAL CIVIL JURISDICTION**

PUBLIC INTEREST LITIGATION NO. OF 2012

In the matter of the public
interest of protecting the rights
of privacy, autonomy, dignity
and free and full enjoyment of
life of the citizens of India,
guaranteed under Articles 19
and 21 of the Indian
Constitution;

AND

In the matter of non-voluntary
and premature implementation
of "Aadhaar" in strict breach of
Article 21 of the Indian
Constitution

AND.

In the matter of excessive
delegation of essential function
without any guidelines, rules or
policy framework in
Notification Dated 29th January
2009 creating the UIDAI

AND

In the matter of potential
breaches of the right to privacy
of citizens of India, through the
means of data collection,
storage and sharing by the
UIDAI, without any legitimate
and rational nexus of improving
the public welfare system

AND

In the matter of standing
committee of the Parliament

Report dated 13th December
2010 rejecting the proposed
National Identification
Authority of India Bill, 2010

1. Vickram Crishma, aged 60 yrs,

Residing at A31 Queens Apts,

Pali Hill, Bandra, Mumbai 400050

E mail. vickramcrishma@gmail.com

2. Kamayani Bali Mahabal, aged 40 years,

Residing at 503, Juhu Bahart CHS,

Gandhi Gram Road,

Juhu, Mumbai 400 059

Email kamayni@gmail.com

3. Yogesh Pawar, aged 43 years,

Residing at 18B/704, Bimbisar Nagar,

Near SRP camp, Western Express Highway,

Goregaon E, Mumbai 65

Email yogeshhp1969@gmail.com

59

4. Dr Nagarjuna G., aged 49 years

Residing at 502, Bhaskara, TIFR Residential Complex,
Homi Bhabha Road, Colaba,
Mumbai 400005
Email ramakumarr@gmail.com

5. Prof. R. Ramkumar, aged 37 years,

Residing at B2/12, Reserve Bank of India,
Officer's Quarters, Chakala,
Andheri-East,
Mumbai 400 093 ...Petitioners
Email nagarjun@gnnowledge.org

Versus

1. UNIQUE IDENTIFICATION AUTHORITY OF INDIA,

Planning Commission,
Government of India,
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

2. Mr. A. B. Pandey.

Deputy Director General, UIDAI,
Mumbai Regional Office,
5th & 7th Floor, MTNL Building,
BD Somani Marg, Cuffe Parade,
Mumbai 400 005

2. The Chairperson, Planning Commission of India,
Yojana Bhavan, Sansad Marg,
New Delhi.

3. National Informatics Centre

Department of Information Technology,
Ministry of Communications and Information Technology,
A-Block, CGO Complex,
Lodhi Road, New Delhi - 110 003 India

4. Union of India

Through the Ministry of Finance
New Delhi.

5. Union of India

Through the Ministry of Home Affairs
New Delhi.

... RESPONDENTS

VAKALATNAMA

To,
Prothonotary & Sr. Master
High Court, O.O.C.J
Mumbai

61

Madam,

We, the Petitioners abovenamed do hereby appoint Mihir Desai,
Advocate, High Court, to act, appear, and plead on my behalf in the
above matter.

IN WITNESS WHEREOF WE HAVE SET AND SUBSCRIBED OUR
HANDS TO THIS WRITING on this 16th day of January, 2012 at
Mumbai.

Accepted



MIHIR DESAI

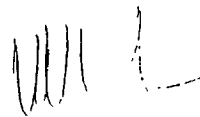
Advocates for the Petitioners

22, Raja Bahadur Mansion

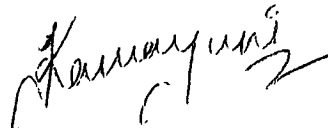
2nd floor, Opp. State Bank of India

Mumbai Samachar Marg

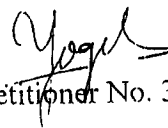
Fort, Mumbai – 400 023.



Petitioner No.1



Petitioner No.2



Petitioner No. 3

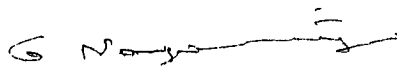
I am not a member of the
welfare Fund, therefore welfare
stamp of Rs 2/- is not affixed
herewith



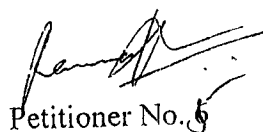
Advocate



Petitioner No.4



Petitioner No.5



Petitioner No.6

IN THE HIGH COURT OF JUDICATURE AT BOMBAY

ORDINARY ORIGINAL CIVIL JURISDICTION

PUBLIC INTEREST LITIGATION NO.

OF 2012

Vickram Crishna & Ors

....Petitioners

Versus

Unique Identification Authority of India & Ors.... Respondents

MEMORANDUM OF REGISTERED ADDRESS

Vickram Crishna

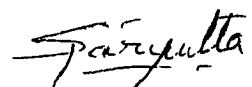
C/o MIHIR DESAI

22, Raja Bahadur Mansion

2nd floor, Opp. State Bank of India

Mumbai Samachar Marg

Fort, Mumbai – 400 023.


Advocate for the Petitioners

IN THE HIGH COURT OF JUDICATURE AT BOMBAY

ORDINARY ORIGINAL CIVIL JURISDICTION

PUBLIC INTEREST LITIGATION NO.

OF 2012

Vickram Crishna & Ors

....Petitioners

Versus


Unique Identification Authority of India & Ors....

Respondents

LIST OF DOCUMENTS

All the documents annexed at **Exhibit A to Exhibit 'T'**

Any other documents relevant for the successful
prosecution.



Advocate for Petitioners

The project that proposes to give every resident a unique identity number is a matter of great concern for those working on issues of food security, NREGA, migration, technology, decentralisation, constitutionalism, civil liberties and human rights. The process of setting up the Authority has resulted in very little, if any, discussion about this project and its effects and fallout. The documents on the UIDAI website, and a recent draft law (the National Identification Authority Bill, which is also on the website) do not provide answers to the many questions that are being raised in the public domain. This project is intended to collect demographic data about all residents in the country. It is said that it will impact on the PDS and NREGA programmes, and plug leakages and save the government large sums of money. It would, however, seem that even basic procedures have not been followed before launching on such a massive project.

Before it goes any further, we consider it imperative that the following be done:

Do a feasibility study: There are claims made in relation to the project, about what it can do for PDS and NREGA, for instance, which does not reflect any understanding of the situation of the situation on the ground.

The project documents do not say what other effects the project may

have, including its potential to be intrusive and violative of privacy, who may handle the data (there will be multiple persons involved in entering, maintaining and using the data), who may be able to have access to the data and similar other questions.

Do a cost-benefit analysis: It is reported that the UIDAI estimates the project will cost Rs 45,000 crores to the exchequer in the next 4 years. This does not seem to include the costs that will be incurred by Registrars, Enrollers, internal systems costs that the PDs system will have to budget if it is to be able to use the UID, the estimated cost to the end user and to the number holder.

In a system such as this, a mere statement that the UIDAI will deal with the security of the data is obviously insufficient. How does the UIDAI propose to deal with data theft? If this security cannot be reasonably guaranteed, the wisdom of holding such data in a central registry may need to be reviewed.

The involvement of firms such as Ernst & Young and Accenture raise further questions about who will have access to the data, and what that means to the people of India.

Constitutionality of this project, including in the matter of privacy, the

relationship between the state and the people, security and other
fundamental rights.

Questions have been raised which have not been addressed so far,
including those about
Undemocratic process. UIDAI was set-up via a GoI notification as an
attached office of the Planning Commission without any discussion or
debate in the Parliament or civil society. In the year and a half of its
inception, the Authority has signed MoUs with virtually all states and
UTs, LIC, Petroleum Ministry and many banks. In July, the Authority
circulated the draft NIA Bill (to achieve statutory status); the window for
public feedback was two weeks. Despite widespread feedback and calls
for making all feedback public, the Authority has not made feedback
available. Further in direct contravention to the process of public
feedback, the NIA Bill was listed for introduction in the Lok Sabha 2010
monsoon session
Privacy (It is only now that the DoPT is said to be working on a draft of a
privacy law, but nothing is out for discussion even yet)
Surveillance: where this technology, and the existence of the UID
number, and its working, could result in increasing the potential for
surveillance

Profiling, Tracking, Convergence, by which those with access to state power, as well as companies, could collate information about each individual with the help of the UID number.

National IDs have been abandoned in the US, Australia and the newly-elected British government. The reasons have predominantly been costs and privacy. If it is too expensive for the US with a population of 308 million, and the UK with 61 million people, and Australia with 21 million people, it is being asked why India thinks it can prioritise its spending in this direction. In the UK, the Home Secretary explained that they were abandoning the project because it would otherwise be 'intrusive bullying by the state, and that the government intended to be the 'servant of the people, and not their 'master. Is there a lesson in it for us? In the late nineties, the Supreme Court of Philippines struck down the Presidents Executive Order A.O 308 which instituted a biometric based national ID system calling it unconstitutional on two grounds the overreach of the executive over the legislative powers of the congress and invasion of privacy. The same is applicable in India UIDAI has been constituted on the basis of a GoI notification and there is a fundamental risk to civil liberties with the convergence of UID, NATGRID etc.

The UIDAI is still at the stage of conducting pilot studies. The biometric pilot study has reportedly already thrown up problems especially among the poor whose fingerprints are not stable, and whose iris scans suffer from malnourishment related cataract and among whom the incidence of corneal scars is often found. The project is clearly still in its inception. The project should be halted before it goes any further and the prelude to the project be attended to, the public informed and consulted, and the wisdom of the project determined. The Draft Bill too needs to be publicly debated. This is a project that could change the status of the people in this country, with effects on our security and constitutional rights, and a consideration of all aspects of the project should be undertaken with this in mind.

We, therefore, ask that:

The project be halted

A feasibility study be done covering all aspects of this issue

Experts be tasked with studying its constitutionality

The law on privacy be urgently worked on (this will affect matters way beyond the UID project)

A cost : benefit analysis be done

A public, informed debate be conducted before any such major change be brought in.

This Statement was issued to the Press on 28th September, 2010 in New

Delhi

List of signatories to the Statement on the UID

Justice VR Krishna Iyer, Retired Judge, Supreme Court of India

satgamaya@dataone.in

Prof Romila Thapar, Historian romila.thapar@gmail.com

K.G.Kannabiran, Senior Civil Liberties Lawyer

kg.kannabiran@gmail.com

Kavita Srivastava, PUCL and Right to Food Campaign

Aruna Roy, MKKS, Rajasthan

Nikhil Dey, MKKS, Rajasthan

S.R.Sankaran, Retired Secretary, Government of India

Deep Joshi, Independent Consultant

Upendra Baxi, Jurist and ex-Vice Chancellor of Universities of Surat and

Delhi BaxiUpendra@aol.com

Uma Chakravarthi, Historian

Shohini Ghosh, Teacher and Film Maker

Amar Kanwar, Film Maker

Bezwada Wilson, Safai Karamchari Andolan

Trilochan Sastry, IIMB, and Association for Democratic Reforms

7c

trilochans@iimb ernet.in

Prof. Jagdeep Chhokar, ex- IIMA, and Association for Democratic

Reforms

Justice A.P.Shah, Retired Chief Justice of High Court of Delhi

ajitprakashshah@gmail.com

True Copy



Adv.

True copy

ENROLMENT FORM (आवृत्त फार्म)



संस्कृत विभाग, भारत सरकार



EXH-B-161112

71

Please use CAPITAL letters: जमा करत नाम पदार्थ

Date (दिनांक) / /

Part A - Primary Details / (प्रथम विवरण)

Name

(पदार्थ)

Mother

Father

Husband

Guardian's Name

(नाम)

(Name of Mother/Father/Guardian is must for children below 5 years of age)

Date of Birth

यदि नहीं तो /

If not known, Age

Gender

Male

Female

Transgender

Co.

House No. and name of the locality

Street No and name of the street

Landmark

Village / City / Town / State

District

State

Pin code

Part B - Additional Information / (अतिरिक्त विवरण)

Phone No. / Mobile No. (optional)

Email (optional)

Part C - Financial Information / (वित्तीय जानकारी)

I want to link my existing bank A/c to Aadhaar and I have no objection on this issue

Bank name and Branch (पदार्थ नाम व शाखा)

A/c No (कलम नंबर)

Unique Identification Authority of India (UIDAI)
Planning Commission, Govt. of India
April, 2010



CREATING A UNIQUE IDENTITY NUMBER FOR
EVERY RESIDENT IN INDIA

UIDAI STRATEGY OVERVIEW



16/01/12

Exh - c

CONTENTS

| | |
|---|-----------|
| Executive Summary | 1 |
| 1 Introduction and historical background | 6 |
| 1.1 Historical background and evolution of the UIDAI project | 6 |
| 1.2 The UIDAI Approach | 9 |
| 2 The UIDAI implementation model | 10 |
| 2.1 The Central Identities Data Repository (CIDR) .. | 10 |
| 2.2 The Unique Identity Number .. | 10 |
| 2.3 The Unique ID agencies | 11 |
| 2.4 Setting standards on demographic data and biometrics | 12 |
| 3 Enrolment into the UID system | 14 |
| 3.1 The enrolment process | 14 |
| 3.2 Enrolment strategy in rural and urban India .. | 16 |
| 3.3 A focused effort to enrol the poor and hard to reach groups | 17 |
| 3.4 Enrolment cost | 19 |
| 3.5 Ensuring clean enrolment data from registrars | 20 |
| 3.6 Updating UID details | 20 |
| 3.7 Reaching critical mass in enrolments | 21 |
| 3.8 Tracking enrolments across the country | 22 |
| 3.9 Reaching a sustainable steady state in enrolments | 23 |
| 4 Ensuring strong authentication and what it means for the UIDAI | 25 |
| 4.1 Enabling UID adoption for authentication | 25 |
| 4.2 Types of authentication | 26 |
| 4.3 Authentication and the UIDAI revenue model | 27 |
| 5 Legal framework | 30 |
| 6 Data security and fraud | 33 |
| 6.1 Protecting personal information of residents .. | 33 |
| 6.2 Fraud scenarios | 34 |
| 7 Technology architecture of the UIDAI | 35 |
| 7.1 System architecture | 35 |
| 8 Project execution | 37 |
| 8.1 Addressing challenges of scale | 37 |
| 9 Project risks | 38 |
| 10 UID-enabled micropayment architecture | 39 |
| 10.1 Features of UID-enabled micropayments | 40 |
| 10.2 Benefits | 41 |
| 10.3 Conclusion | 42 |

Executive Summary

Overview

In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence.

As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

Such duplication of effort and 'identity silos' increase overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes.

There are clearly, immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies.

A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent

themselves differently to different agencies. This will result in significant savings to the state exchequer.

The UIDAI - evolving an approach to identity

The Government of India undertook an effort to provide a clear identity to residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently in 2003, the Government approved the Multipurpose National Identity Card (MNIC).

The Unique Identification Authority of India (UIDAI) was established in January 2009, as an attached office to the 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's approach will keep in mind the learnings from the government's previous efforts at issuing identity.

Executive Summary

Overview

In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence.

As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

Such duplication of effort and 'identity silos' increase overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes.

There are clearly, immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies.

A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent

themselves differently to different agencies. This will result in significant savings to the state exchequer.

The UIDAI – evolving an approach to identity

The Government of India undertook an effort to provide a clear identity to residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently in 2003, the Government approved the Multipurpose National Identity Card (MNIC).

The Unique Identification Authority of India (UIDAI) was established in January 2009, as an attached office to the 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's approach will keep in mind the learnings from the government's previous efforts at issuing identity.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives. The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

Features of the UIDAI model

The Unique Identification number (UID) will only provide identity: The UIDAI's purview will be limited to the issue of unique identification numbers linked to a person's demographic and biometric information. The UID will only guarantee identity, not rights, benefits or entitlements.

The UID will prove identity, not citizenship: All residents in the country can be issued a unique ID. The UID is proof of identity and does not confer citizenship.

A pro-poor approach: The UIDAI envisions full enrolment of residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the UIDAI plans to partner with – the NREGA, RSBY, and PDS – will help bring large numbers of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor.

Enrolment of residents with proper verification: Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean from the start of the program.

However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The UIDAI will ensure that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.

A partnership model: The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central Identities Data Repository (CIDR), which will issue UIDs, update resident information, and authenticate the identity of residents as required.

In addition, the UIDAI will partner with agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI. Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or will appoint agencies as enrollers, who will interface with people seeking UID numbers. The Authority will also partner with service providers for authentication.

The UIDAI will emphasize a flexible model for Registrars: The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR (Know Your Resident) verification, collecting demographic data on residents for their specific requirements,

and in authentication. The UIDAI will provide standards to enable Registrars maintain uniformity in collecting certain demographic and biometric information, and in basic KYR. These standards have been finalized by the Demographic Data Standards and Verification Procedures Committee and Biometric Standards Committees which was constituted by the UIDAI constituted.

Enrolment 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. This will not however, preclude governments or Registrars from mandating enrolment.

The UIDAI will issue a number, not a card: The UIDAI's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar.

The number will not contain intelligence: Loading intelligence into identity numbers makes them susceptible to fraud and theft. The UID will be a random number.

The UIDAI will only collect basic information on the resident: The UIDAI will seek the following demographic and biometric information in order to issue a UID number:

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

Process to ensure no duplicates: Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to ensure that no duplicates exist.

The incentives in the UID system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have only one chance to be in the database, individuals will provide accurate data. This incentive will become especially powerful as benefits and entitlements are linked to the UID.

Online authentication: The UIDAI will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and agencies in adopting the UID authentication process, and will help define the infrastructure and processes they need.

77

The UIDAI will not share resident data: The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity only through a 'Yes' or 'No' response.

Technology will undergird the UIDAI system: Technology systems will have a major role across the UIDAI infrastructure. The UID database will be stored on a central server. Enrolment of the resident will be computerized, and information exchange between Registrars and the CIDR will be over a network. Authentication of the resident will be online. The Authority will also put systems in place for the security and safety of information.

Benefits

For residents: The UID will become the single source of identity verification. Once residents enrol, they can use the number multiple times - they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on.

By providing a clear proof of identity, the UID will also facilitate entry for poor and underprivileged residents into the formal banking system, and the opportunity to avail services provided by the government and the private sector. The UID will also give migrants mobility of identity.

For Registrars and enrollers: The UIDAI will only enrol residents after de-duplicating their records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower KYR costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate. The strong authentication that the UID number offers will improve services, leading to better resident satisfaction.

For Governments: Eliminating duplication under various schemes is expected to save substantial money for the government exchequer. It will also provide governments with accurate data on residents, enable direct benefit programs, and allow government departments to coordinate investments and share information.

Revenue Model

By providing identity authentication, the UIDAI will be taking on a process that costs agencies and service providers hundreds of crores every year. The Authority will evolve suitable policies on the issue of charging a fee for its authentication services, which will offset its long-term costs. Registrars and service providers will also be able to charge for the cards they issue residents with the UID number. Such pricing will be within UIDAI guidelines.

78

Timelines

The UIDAI will start issuing UIDs between August 2010 and February 2011, and plans to cover 600 million people within 4 years from the start of the issuing of the first set of UIDs. This can be accelerated if more Registrars partner with the UIDAI for both enrolment and authentication. The adoption of UIDs is expected to gain momentum with time, as the number establishes itself as the most accepted identity proof in the country.

Conclusion

India will be the first country to implement a biometric-based unique ID system for its residents on such a large scale. The UID will serve as a universal proof of identity, allowing residents to prove their identity anywhere in the country. It will give the government a clear view on India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments, and monitor money and resource flows across the country.

The timing of this initiative is encouraging – the creation of the UIDAI coincides with growing social investment in India, a shift in focus to direct benefits, and with the spread of IT and mobile phones, which has made the public receptive to technology-based solutions. The UIDAI is committed to making this project a success. An initiative of this magnitude will also require the active participation of central, state and local governments, as well as public and private sector agencies across the country. With their support, the project will help realize a larger vision of inclusion and development for India.

1

Introduction and historical background

A crucial factor that determines an individual's well-being in a country is whether their identity is recognized in the eyes of the government. Weak identity limits the power of the country's residents when it comes to claiming basic political and economic rights. The lack of identity is especially detrimental for the poor and the underprivileged, the people who live in India's "social, political and economic periphery". Agencies in both the public and private sector in India usually require a clear proof of identity to provide services. Since the poor often lack such documentation, they face enormous barriers in accessing benefits and subsidies.

For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats.

However in India, the goal of issuing a universally used, unique identity number to each resident poses a significant challenge. A project of this scale has not been attempted anywhere in the world, and requires an innovative model, distinct from what we have witnessed in identity systems so far anywhere in the world.

1.1 Historical background and evolution of the UIDAI project

The Unique identification project was initially conceived by the Planning Commission as an initiative that would provide a clear and unique identity number for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

The concept of unique identification was first discussed and worked upon since 2006 when administrative approval for the project – "Unique ID for BPL families" was given on March 3rd, 2006 by the Department of Information Technology, Ministry of Communications and Information Technology. This project was to be implemented by the NIC over a period of 12 months. Subsequently, a Processes Committee to suggest processes for updation, modification, addition and deletion of data fields from the core data base to be created under the Unique ID for BPL families Project was set up on July 3rd 2006.

A "Strategic Vision on the UID Project" was prepared and submitted to this Committee. It envisaged the close linkage that the UID would have to the electoral database. The Committee also appreciated the need of a UID Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the Authority and at the same time enable a focused approach to attaining the goals set for the XI Plan. The Seventh

Meeting of the Process Committee on 30th August 2007 decided to furnish to the Planning Commission a detailed proposal based on the resource model for seeking its "in principle" approval.

At the same time, the Registrar General of India was engaged in the creation of the National Population Registrar and issuance of Multi-purpose National Identity Cards to citizens of India.

Therefore, it was decided, with the approval of the Prime Minister, to constitute an Empowered Group of Ministers (EGoM) to collate the two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number project of the Department of Information Technology. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these. The EGoM was constituted on December 4th, 2006.

The **first meeting of the EGoM** was held on November 27th, 2007. It recognised the need for creating an identity related resident database, regardless of whether the database is created based on a de-novo collection of individual data or is based on already existing data such as the voter list. It also recognised that there is a crucial and imperative need to identify and establish an institutional mechanism that will "own" the database and will be responsible for its maintenance and updating on an ongoing basis, post its creation.

The **second meeting of the EGoM** was held on January 28th, 2008. It decided on the strategy for the collation of NPR and UID. Inter-alia, the proposal to establish UID Authority under the Planning Commission was approved.

The **third meeting of the EGoM** was held on August 7th, 2008. The Planning Commission had placed before the EGoM a detailed proposal for setting up the UIDAI. The meeting decided that certain issues raised by the members with relation to the UIDAI would need to be examined by an official level committee. It referred the matter to a Committee of Secretaries to examine and give its recommendations to the EGoM to facilitate a final decision.

Subsequent to the Committee of Secretaries recommendations, the **fourth meeting of the EGoM** was held on November 4th, 2008. The recommendations of the Committee of Secretaries was presented to the EGoM and the following decisions were taken:

- a) Initially the UIDAI may be notified as an executive authority, and investing it with statutory authority could be taken up for consideration later at an appropriate time.
- b) UIDAI may limit its activities to the creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.
- c) UIDAI will take its own decision as to how to build the database.
- d) UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.

- e) Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure through the DoE/CCEA.
- f) Approval to the constitution of the State UID Authorities simultaneously with the Central UIDAI with a core team of 3 personnel.
- g) December 2009 was given as the target date for UID to be made available for usage by an initial set of authorized users.
- h) Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed organizational structure, staff and other requirements.

1.1. Subsequently, on January 22nd, 2009 the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers considered the proposal submitted by the Department of Information Technology regarding the governance structure and recommended that

- a) The notification for constitution of the UIDAI should be issued immediately.
- b) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission to be constituted to oversee the work of the authority.
- c) A Member, Planning Commission or the Secretary, Planning Commission may be also assigned the task of looking after the work proposed of the Chief UID Commissioner.
- d) Core Team to be put in place.

In pursuance of the Empowered group of Ministers' fourth meeting dated November 4th, 2008, the **Unique Identification Authority of India** was constituted and notified by the Planning Commission on January 28th, 2009 as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. The role and responsibilities of the UIDAI was laid down in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UID scheme, and shall own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis.

Subsequently on July 2nd, 2009 Shri Nandan Nilekani was appointed as the Chairman of the UIDAI. Shri Nilekani assumed charge on 23rd July, 2009 and since then the UIDAI has started functioning.

The Prime Minister's Council on UID Authority was constituted on 30th July, 2009 and its first meeting had taken place on 12th August, 2009. The Council endorsed the broad approach submitted by the UIDAI.

Subsequently, the Government constituted a **Cabinet Committee on Unique Identification**

Authority of India vide its order no 1/11/6/2009 dated 22nd October, 2009. The functions of this Committee, as per this notification are: All issues relating to the Unique identification Authority of India including its organisation, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

1.2 The UIDAI approach

In 2007, the Planning Commission had recommended an approach to issuing unique identification numbers, where the enrolment into a Unique Identification (UID) database could be speeded up by using existing resident records in the databases of the Election Commission, PAN etc. This approach would speed up enrolment for those residents present in one of the aforementioned databases. These databases however, may contain inaccuracies.

The model envisioned by the Unique Identification Authority of India (UIDAI) takes into account the inputs of the Planning Commission, as well as learnings from the previous approaches to identity. The detailed approach and the model of implementation is explained in subsequent chapters.

2

The UIDAI implementation model

The model that the UIDAI envisions will have the reach and flexibility to enrol residents across the country.

The UIDAI, as a statutory body, will be responsible for creating, administering and enforcing policy. The UIDAI will prescribe guidelines on the biometric technology, the various processes around enrolment, and verification procedures to be followed to enroll into the UID system. 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.

2.1 The Central Identities Data Repository (CIDR)

The CIDR will be the central data repository, and will function as a Managed Service Provider. It will implement the core services around the UID - 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:

2.2 The Unique Identity Number

The Unique ID or UID will be a numeric that is unique across all 1.2 billion residents in India.

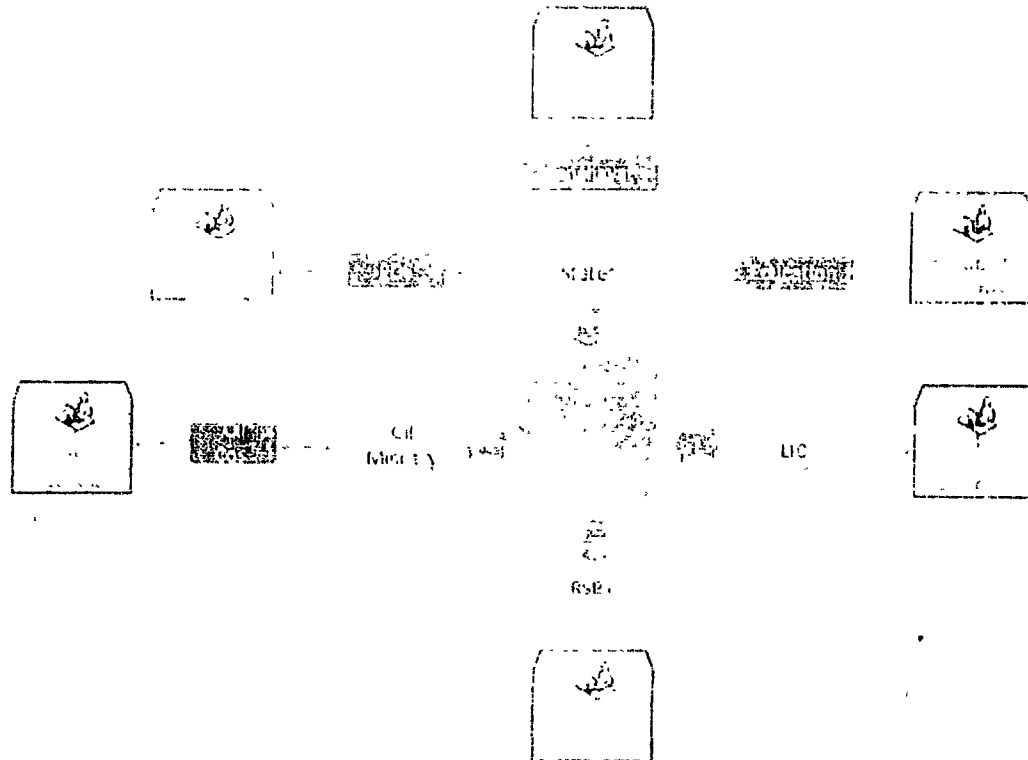
The UID number will not contain intelligence. In older identity systems, it was customary to load the ID number with information related to the date of birth, as well as the location of the person. However this makes the number susceptible to fraud and theft, and migration of the resident quickly makes location details out of date. The UID will be a random number.

The UIDAI will also be collecting the following data fields and biometrics for issuing a UID:

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

2.3 The Unique ID agencies

The UIDAI will partner with a variety of agencies and service providers to enrol residents for UID numbers and verify their identity.



The structure of these UID agencies will be as follows:

Registrars – Registrars will be State governments or central government agencies such as the Oil Ministry and LIC. Registrars may also be private sector participants such as banks and insurance firms.

The UIDAI will enter into memorandum of understandings' (MoUs) with individual Registrars, and enable their on-boarding into the UID system. The Registrars will need to make changes to their processes to be UID-ready. The UIDAI will support them in this, and in linking to the CIDR, connecting to the UID system, and adding UID fields to their databases.

The Registrar will take on the responsibility of ensuring that clean and correct data flows into the CIDR. Their key role in the system will be in aggregating enrolments from sub-registrars and enrolling agencies and forwarding it to the CIDR. Each Registrar will adopt UIDAI standards in the technology used for biometrics, as well as in collecting and verifying resident information, and submitting to audits.

The UIDAI will also enter into agreements with some Registrars for using the CIDR solely for authentication purposes. The service providers who will adopt the UID system for identity authentication during service delivery will follow certain processes and standards, and may need to re-engineer their internal processes.

Sub-Registrars – These will be the departments/entities that report to a specific Registrar. For instance, the line departments of the state government such as the RDPR (Rural Development and Panchayati Raj) department would be sub-registrars to the state government Registrar.

Enrolling Agencies – Enrolling agencies will directly interact with and enrol residents into the CIDR. For example, the hospital where a baby is born would be the 'enrolling agency' for the baby's UID, and would report to the municipality sub-registrar.

Outreach Groups – The UIDAI along with the Registrars will also partner with civil society groups and community networks which will promote the UID number and provide information on enrolment for hard to reach and marginalised populations.

2.4 Setting standards on demographic data and biometrics

The UIDAI's approach relies on the uniformity of standards in certain vital areas of operation. The Demographic data fields and verification procedure in the UID system as well as the Biometric standards to be utilized need to be standardized across the country and across the various registrars in the UID system. This is a sine qua non for the operability of the system. Hence, the UIDAI established two Committees to look into the issue of standards.

Committee on Demographic Data Standards and Verification Procedures

The UIDAI had constituted a Committee headed by Mr. N. Vittal, former CVC on 9th October 2009 to go into the question as to what demographic details should be collected from the residents for assigning of unique IDs. The Committee was also to go into the question as to what should be the process of verification of the residents at the time of their enrolment into the UID system. The mandate of the Committee was crucial because it is necessary to ensure that the integrity and correctness of the data is not compromised while ensuring that the process of verification is non-harassing to individuals. The Committee was mandated to give its report within 90 days of its constitution. However, it submitted its report on 9th December 2009, well before the ninety days' period given to it. The Report of the Committee has been accepted by the Authority. The Committee recommended the following data fields : Name, Date of birth, Gender, Father's/ Husband's/ Guardian's name and UID (optional for adult residents), Mother's/ Wife's/ Guardian's name and UID (optional for adult residents), Introducer's name and UID (in case of lack of documents) and Address. It has also specified the verification process which broadly falls into three categories (i) Document-based, (ii) Introducer-based (in case of lack of documents) and (iii) Community-based verifications, a process which will be followed during the creation of NPR. The Report of the Vittal Committee is available at www.uidai.gov.in

Committee on Biometric Standards

As biometric attributes of the residents are going to be used as the basic signature for de-duplication and to ensure uniqueness, it is necessary to go into the question as to what should be the type and specifications of biometrics to be collected at the time of enrolment. Therefore, a Biometrics Standards Committee, under the Chairmanship of the Director General of NIC, Dr. BK Gairola was constituted by the Authority on 29th September, 2009. This Committee was also expected to give its report within 90 days of its constitution. The Report was submitted on 7th January, 2010. The UIDAI has examined their Report and has accepted the standards for various biometric attributes as recommended by the committee as also various other recommendations related to collection of biometrics and their quality. The UIDAI has also decided that the face, all ten finger prints and both iris scans should be collected at the time of capturing the demographic and biometric details of a resident. This will be able to ensure uniqueness of the IDs at a scale of 1.2 billion residents. The report of the biometric committee is also available at www.uidai.gov.in

The UIDAI was declared as an Apex body to set standards in the areas of biometric and demographic data standards by the Prime Minister's Council of UIDAI. Now that both these standards have been finalized by the UIDAI, these standards/specifications, processes and systems will be used by all the registrars to for enrolment of the residents into the UID system.

3

Enrolment into the UID system

A critical aspect of the UID enrolment process is that enrolment will not be through a mandate, but will be demand driven. The momentum for the UID will come from residents enrolling in order to access the benefits and services associated with it.

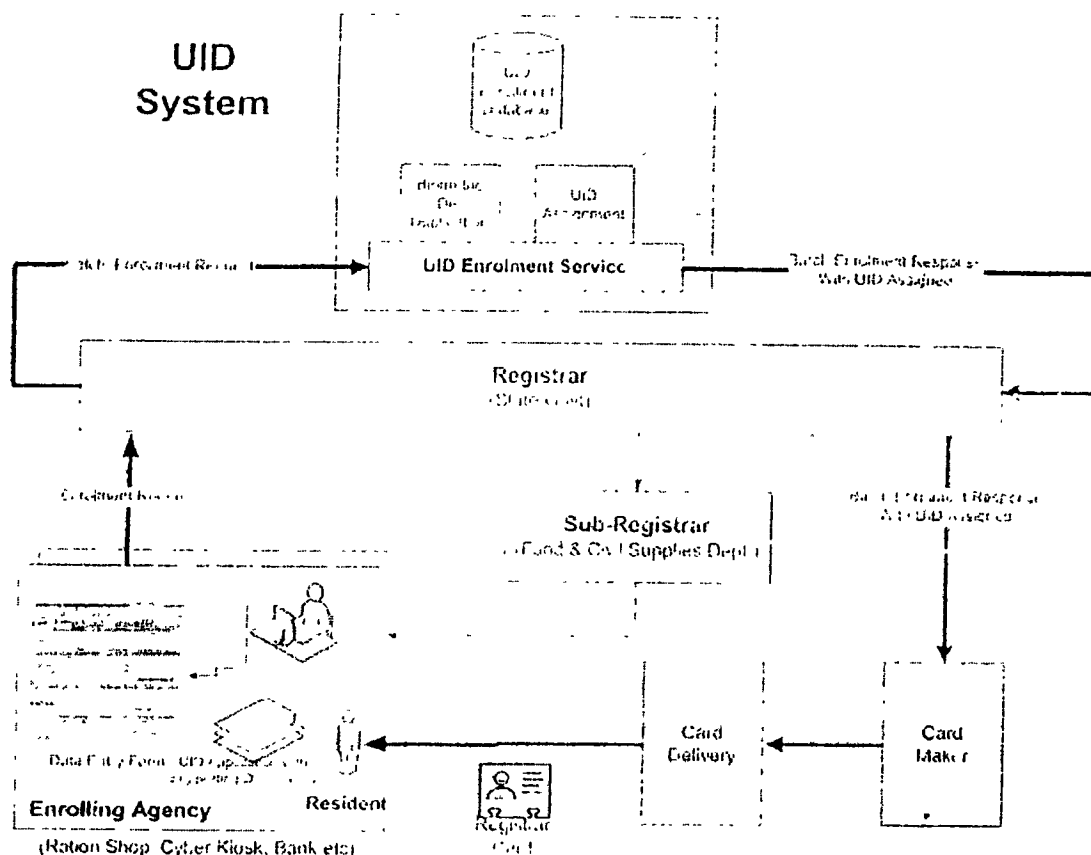
The basic advantage of the UID that can drive this demand, which will be communicated while promoting enrolment, is that the UID will be one number, which can be used to prove identity for life. Once the resident gets the unique ID, it may be accepted as identity proof across service providers.

3.1 The enrolment process

The enrolment process for the UID number will begin with a resident submitting his/her information to the enrolling agency with supporting documents. This information will be verified according to the prescribed verification procedure as per the DDSVP Committee Report. To make sure the poor are not excluded, the UIDAI has prescribed guidelines for applicants without documents.

Once the enroller verifies the resident's information, it will submit the application request – either singly or in batches – through the Registrar to the CIDR. The CIDR will then run a de-duplication check, comparing the resident's biometric and demographic information to the records in the database to ensure that the resident is not already enrolled.

Since de-duplication also compares biometric records, it would catch individuals enrolling with a different set of demographic details. The fact that the UID system is both de-duplicated and universal will discourage residents from giving incorrect data at the time of enrolment.



Issuing the UID number

Once the UID number is assigned, the UIDAI will forward the resident a letter which contains his/her registered demographic and biometric details. This letter may also have a tearaway portion which has the UID number, name, photograph and a 2D barcode of the finger print minutiae digest. If there are any mistakes in the demographic details, the resident can contact the relevant Registrar/enrolling agency as per a prescribed procedure.

If the Registrar issues a card to the resident, the UIDAI will recommend that the card contain the UID number, name and photograph. They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/ store the biometric collected from the applicant on the issued card. If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification. But the UIDAI will not insist on, audit or enforce this.

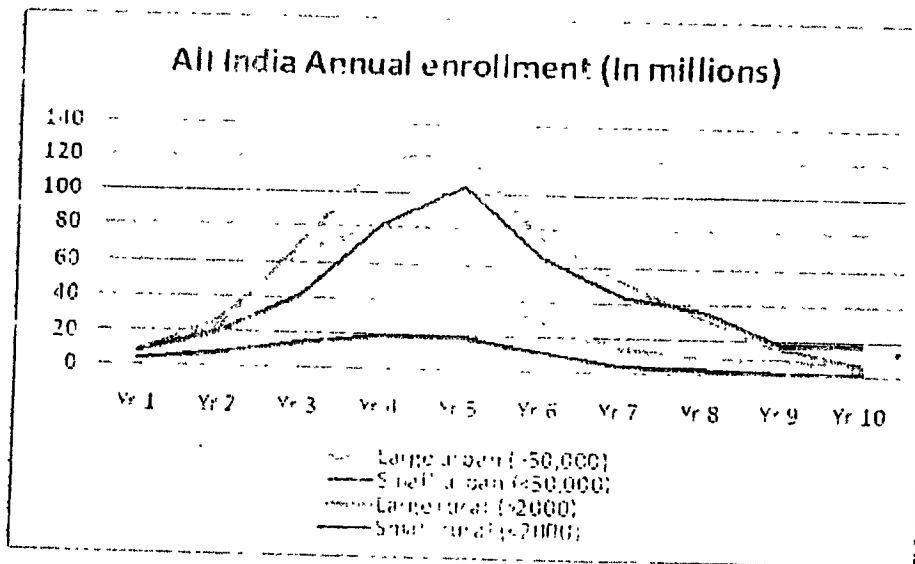
All data entry that the enrolling agencies take up on behalf of the Registrars will be done in English. It can then be converted into the local language using standard transliteration software, and verified for accuracy by the Registrar. The letter the UIDAI sends the resident will consequently

89

contain all demographic details in English as well as the local language of the state in which the resident resides. In this regard, the UIDAI will follow the precedent set by the Election Commission of India.

3.2 Enrolment strategy in rural and urban India

The approach of the UIDAI to enrolment will be a pro-rural/pro-poor one. The Registrars targeted for rural India – the NREGA, PDS, Social security pensions – will be government agencies with large rural networks and significant bases among the poor. As a result, the UIDAI expects initial enrolment to be fairly rapid in both large and small rural areas.



The enrolment strategy for urban India will include organizations which dominate services for urban residents, such as LIC and Passports. The table below summarizes the Registrars who are

| UID Registrar | Primary Access ¹ | Additional Access ² | Potential Overlap | Effective Enrolment |
|----------------------|-----------------------------|--------------------------------|-------------------|---------------------|
| Crore Residents | | | | |
| LPG (Oil PSU) | 8.4 ³ | 16.8 ⁴ | 20% | 20.2 |
| LIC (Life Insurance) | 13.5 | 13.5 | 50% | 13.5 |
| PAN Cards | 4.0 | - | 75% | 1.0 |
| Passports | 6.0 | - | 80% | 1.2 |
| Urban Enrolment | | | | 35.9 |
| Lic (Life Insurance) | 3.5 | 3.5 | 90% | 0.7 |
| NREGA | 10.0 | 20.0 | 10% | 27.0 |
| BPL Ration Cards | 7.0 | 21.0 | 60% | 11.2 |
| State BPL/APL | 15.0 | 45.0 | 50% | 30.0 |
| Old Age Pensioners | 1.5 | 1.0 | 70% | 0.8 |
| Women/Child Welfare | 1.0 | 2.0 | 70% | 0.9 |
| Social Welfare | 1.0 | 2.0 | 70% | 0.9 |
| RSBY | 0.5 | 1.0 | 70% | 0.5 |
| Rural Enrolment | | | | 72.0 |
| Total Enrolment | | | | 107.9 |

In addition to these enrollers, 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 enrol 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.

3.3 A focused effort to enrol the poor and hard to reach groups

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.

¹These are residents who are part of the Registrar's customer / subsidiary beneficiary database and can be mandated to provide their UID

²The residents under additional access are family members who can be easily covered while enrolling the primary residents. These can be all family members in the case of LPG connections and the nominees in case of LIC Policies.

³The total number of gas connections is 10.51 crores, and this estimates that there are 20% ineligible connections

⁴Assuming there are an average of three members in each family having a gas connection from an Oil PSU

Urban Poor

The urban poor are among the most ignored and disadvantaged people in India. The main challenges in enrolment here exist because this group consists mainly of migrant workers with temporary or seasonal jobs. 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 the family or business to enable these members (who are co-residents/co-workers) to get enrolled into the UID with the same address proof the business or family uses. There can be a host of financial incentives offered to enrol such co-residents.

Financial institutions: The urban poor often borrow from micro-finance institutions and other sources and these could serve as enrolment points for them. There are established chit funds that can also act as enrolment points for the UID to improve coverage.

NGCs and Non-profits: There are several established non-profits working in urban slums in education, healthcare and social empowerment. They can be used to educate the poor on the benefits of the UID, for actual enrolment and to help endorse identity for people who lack documentation.

Children

India is a young country with over 400 million residents below the age of 18. While family-based government schemes will as Registrars, help enrol children, this population may need to be specifically targeted.

ICDS: ICDS is one of the world's largest integrated early childhood programs, with over 40,000 centers nationwide. The program covers over 5 million expectant and nursing mothers and 25 million children under the age of six. These centers can be information or enrolment points for non-school going children.

School admission: It may be mandated that at the time of joining school (first standard) it is necessary for children to have a UID or to enrol for one. This way the child can be tracked for progress and targeted for direct benefits.

The SSA program could also help enrol children in the 6-14 age group into the UID, which would also enable better child tracking and improvements in the mid-day meal schemes.

For children, the advantages from the UID would be significant. Child-related programs in India have relied on often inaccurate, aggregate data at school/cluster/block levels, making these programs ineffective. The concept of Universal Child Tracking – the ability to track every child and ensure their all round development – is gaining ground. An accurate database of children with UIDs would be immensely beneficial to programs within the Women and Child welfare as well as the Education departments, which track development in anganwadis and progress of children in government schools, and work to eliminate child labor.

Women

Apart from enrollers that are family-based government services in both urban and rural India such as PDS, RSBY etc, there needs to be a strategy to cover women outside this net:

Financial institutions: Robust collectives of women exist within micro-finance institutions and self-help groups across the country. These would be important enrolment points for women.

Organizations like Mahila Samakhya in the 9 states of Karnataka, Kerala, Andhra Pradesh, Gujarat, Uttar Pradesh, Uttar Khand, Assam and Jharkhand. They work in several thousand villages to help women and can act as touch points for education or enrolment of women.

The National Commission for Women: This is the apex national level organization of India for protecting and promoting the interests of women. They have a massive outreach program that can reach out to disadvantaged women and get them to enrol. The UID can subsequently be used as a unique handle for a variety of services to be rendered to these women.

Differently-abled people

It is estimated that India has over 60 million differently-abled people, and identity for this population is a massive challenge. The Disability Act of 1995 mandates a certain percentage of employment for the differently-abled, but without the clear identification of such individuals, it is difficult to enforce the law. There is an obvious incentive for organizations like National Center for Promotion of Employment for Disabled People (NCPEDP) to promote the UID, and enable residents with disability to register for a range of benefits. The NGOs and rights groups associated with NCPEDP would also be good mechanisms to reach out to this section of the population.

Tribals

India has a significant tribal population of approximately 90 million tribals, mostly concentrated along a few states. The Government has many programs for the 697 notified tribes, which can be used for enrolment and information dissemination. In addition, NGOs and governments in states with high tribal populations can be Registrars for tribal groups.

The above mentioned approaches are merely indicative of the strategy that the UIDAI will follow to reach marginalized groups. In addition, the UIDAI will reach out to other marginalized groups such as homeless people, individuals in shelter homes, remand homes, asylums, etc.

Civil Society Outreach strategy

3.4 Enrolment costs

Enrolment costs can be thought of in two ways. One will be the cost to the enrolling agencies/Registrars for carrying out the enrolment process. The other costs will be to the residents to come to the enrolment stations. Poor may have to forego their wages for a day and also spend some travel costs to travel to the enrolment stations. The enrolment strategy will explore the

possibility of various mechanisms for funding the enrolment costs. The Registrars have the option here of charging for the cards they issue residents to offset enrolment costs. The UIDAI may issue guidelines around such pricing.

3.5 Ensuring clean enrolment data from Registrars

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 would be on a random sample of residents, carried out either directly by the Authority or through appointed agencies. The audit might focus on:

Verification against scanned documents – The data contained in the resident records will be verified against the scanned documents.

Physical document verification – The physical documents that are held by the Registrar will be validated against the electronic copies.

Periodic process audits – Periodic audits will be carried out to at the enrolment sites, of the processes and software.

3.6 Updating UID details

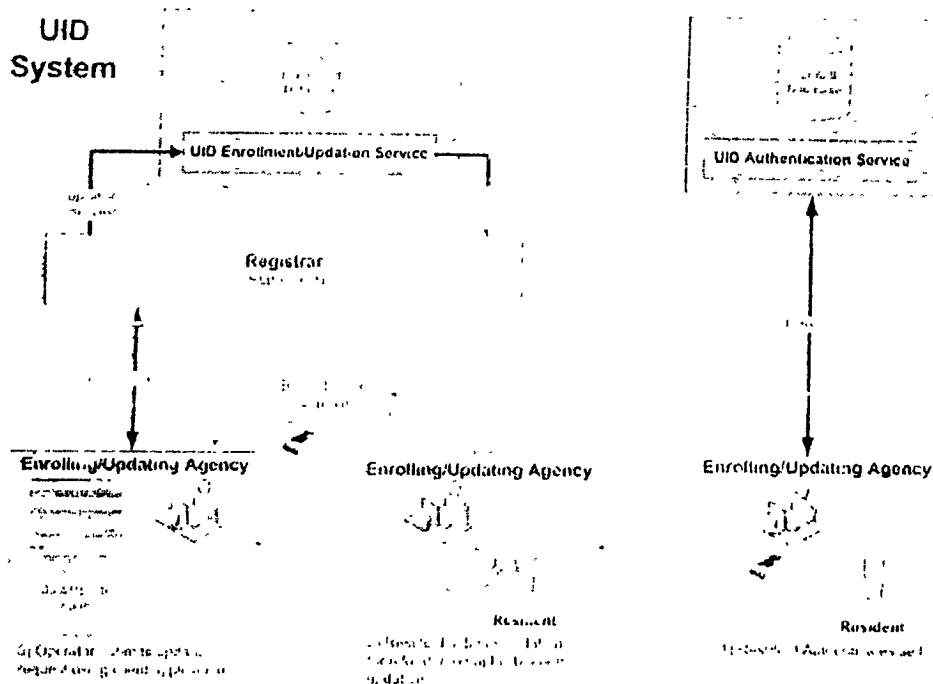
Updating information with the UIDAI

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.

From time to time, the demographic information that the CIDR holds on the resident may also become outdated. Fields that are susceptible to change could be the 'present address' field, as well as the resident's name (after marriage). There might also be an error in the fields that occurred during enrolment into the UID.

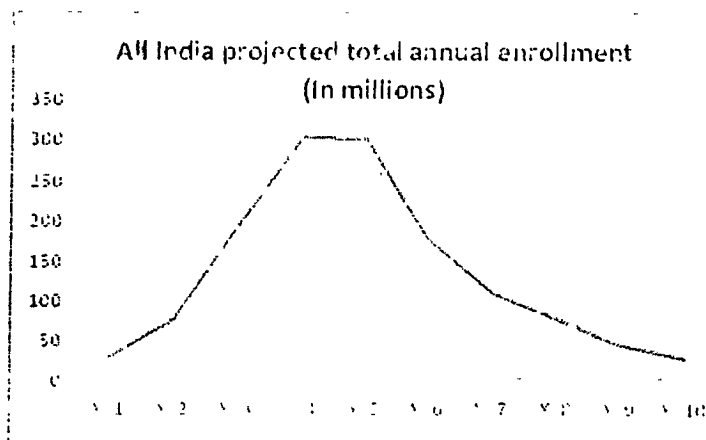
If a service provider authenticating or enrolling a resident finds, through its KYR process that the information provided by the resident (address, name, etc.) does not match with the UID record, or that the biometrics need to be renewed, it can ask the resident to update their information in the UID database. The service provider may make the update a condition for the resident to receive the service/benefit.

Enrolling agencies and Registrars can serve as points where the resident can update their UID fields. The resident will have to submit their new information at these updation points with the required documentary evidence. This may also include a biometric authentication prior to processing the request.



3.7 Reaching critical mass in enrolments

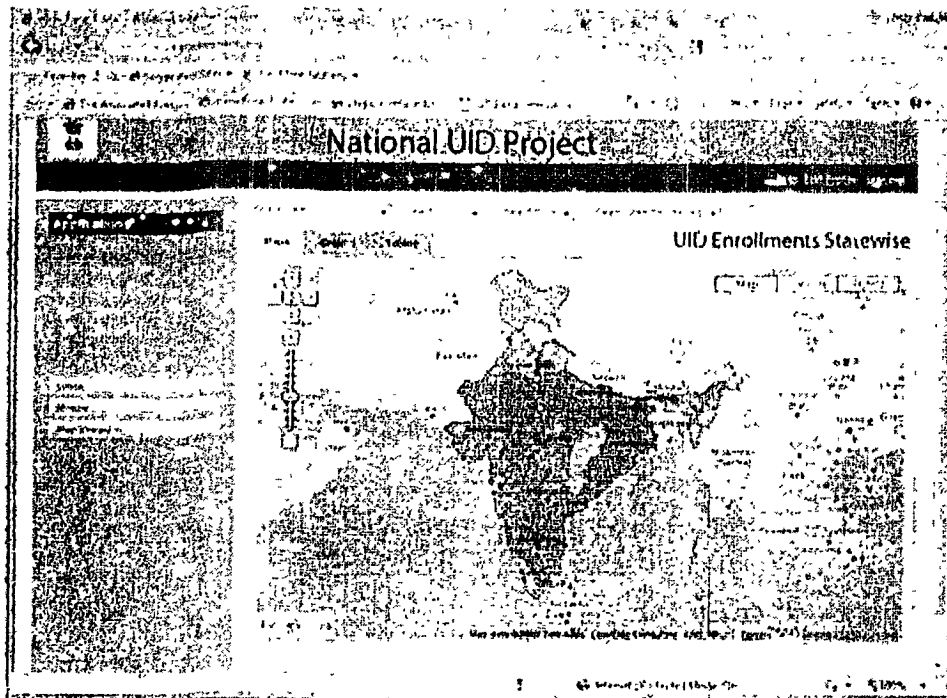
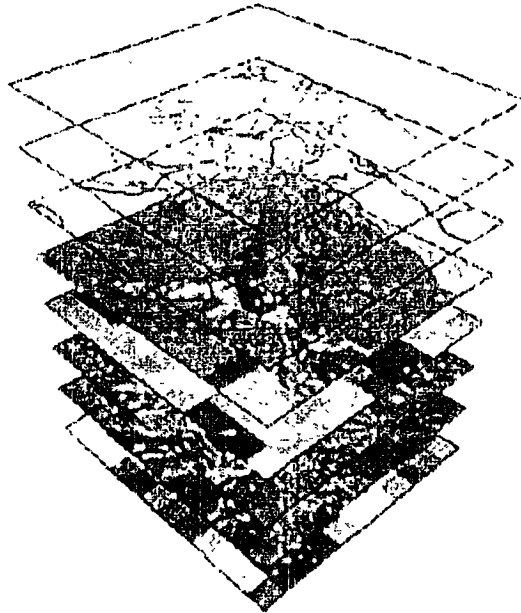
The Authority expects to start issuing the first set of UIDs between August 2010 to February 2011, and enrolment for the UID number is expected to reach a critical mass of around 200 million residents in two to three years. Until this point, the UIDAI will have to focus on generating demand from both Registrars and residents. However, once the critical mass is achieved, it will generate a network effect that drives demand and accelerates adoption among service providers and residents. And as more service providers across the country require the UID to dispense their services and benefits, adoption will ramp up rapidly. In four years, the UIDAI estimates that it will issue 600 million UID numbers.



95

3.8 Tracking enrolments across the country

The UIDAI will employ a GIS Internet-based visual reporting system to track enrolment trends and patterns across India, as the project is rolled out across various Registrars and states.



The GIS system will show all UID enrolments by state, as well as by Registrar. The system will also be able to drill down within states and into districts.

3.9 Reaching a sustainable, steady-state in enrolment

A challenge for full enrolment is registering the approximately 60,000 babies that are born in the country every day. Over the next several years, the UIDAI expects to enrol close to the entire Indian population. Once that goal is achieved, enrolment will reach a steady state, where only births (and deaths) as well as immigrants need to be recorded.

There are however, some challenges in registering new births. First, since their biometrics is not stable, they have to be re-scanned at a later age. Second, names are often not given in India at the time of birth registration.

The UID in the birth certificate

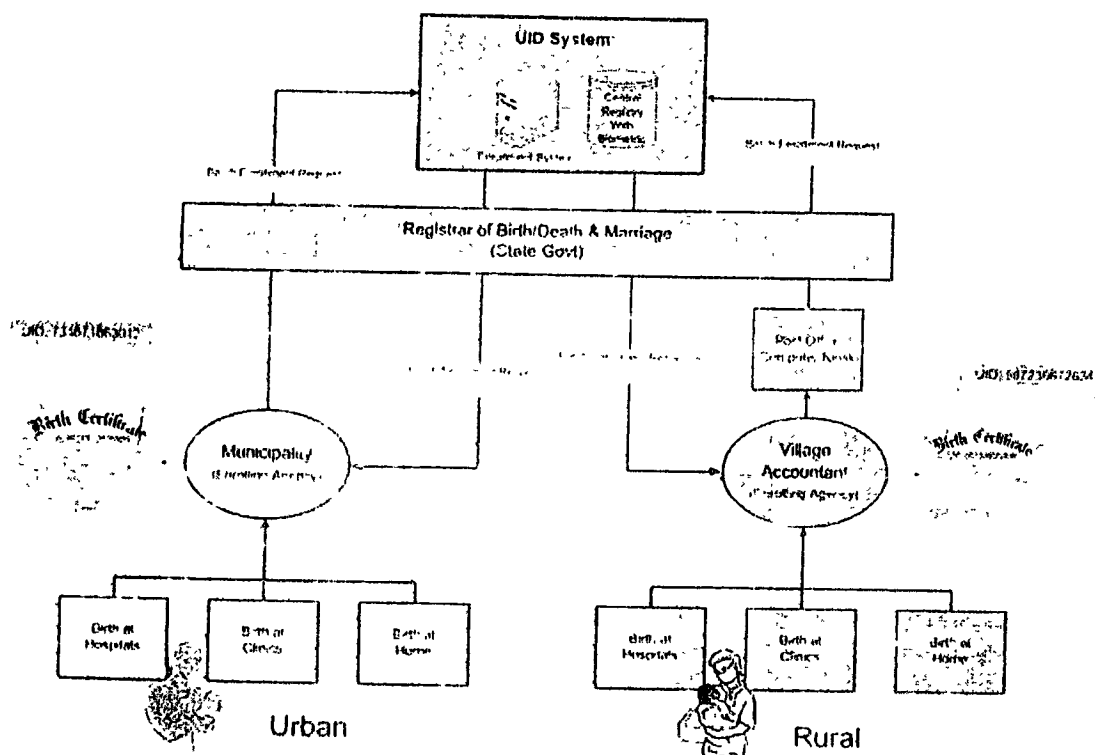
One way to ensure that the UID number is used by all government and private agencies is by inserting it into the birth certificate of the infant. Since the birth certificate is the original identity document, it is likely that this number will then persist as the key identifier through the individual's various life events, such as joining school, immunizations, voting etc.

Since the name is a mandatory field in the UID database, it is essential that the child be given a name before applying for the UID number. This would ensure that the UID can also be allotted at birth.

In the case of urban births, the municipality will be the enrolling authority and the UID Registrar can be the 'Registrar of Births, Deaths and Marriage' at the state level.

In rural areas, births take place at district or block level hospitals, in health care centers and at homes in the village. The village accountant is the Registrar of rural births, and he/she also issues the birth certificate and updates the information through an enrolling agency.





Biometrics and infants

The recording of unique individual biometrics in the UID database is a challenging one for infant records. The solution to this is to record the UID and biometric of the parents in the child's record.

The child's biometrics need to be taken at around 5 years of age, and updated in the UID system every 5 years until the age of 18. This will be enforced by an expiry date attached to the UID number, which will become invalid after that date. Until the time the biometric of the child stabilizes, any one of the parents/guardian will need to provide their biometric information for authentication.

Recording deaths in the UID system

It is also necessary to record deaths in the country, and the birth and death registration act provides for such registration. The same institutions that record births can be in charge of updating deaths in the UID system. The UID system will not remove a record upon the person's death; it will simply mark it as 'deceased' and hence will render it inactive for the purposes of authentication.

4

Ensuring strong authentication, and what it means for the UIDAI

The real test of reliability for the UID system will be during identity authentication. Confirming 'you are who you say you are' remains the primary, often elusive goal of all identity systems.

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 UIDAI will support the Registrars in building the infrastructure and systems necessary to authenticate residents in different parts of the country. This will be especially critical for Registrars working in rural areas and among the poor.

4.1 Enabling UID adoption for authentication

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 indispensable 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 programs 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.

A clear adoption process can overcome this gap by helping introduce the UID method of authentication at every point of service delivery. To ensure this, the UIDAI will not only work with Registrars who do enrolment, but also with non-enrolling, service delivery agencies. Such agencies involved in the delivery of services and benefits will be encouraged to partner with the UIDAI for authentication. Once they authenticate a resident's identity against the UID database every time they carry out a service transaction, they will be able to deliver services far more effectively.

In order to accommodate this authentication, agencies may need to re-engineer their business processes to be UID-enabled. The most basic requirement for change will be in incorporating the UID method of authentication into their systems. Agencies will have to adhere to norms and procedures specified by the UIDAI for fingerprint capture and verification, and introduce a robust biometric authentication process at every point of sale.

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.

The UIDAI is only in the identity domain. The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies – the job of tracking distribution of food grains among BPL families for example, will remain with the state PDS department. The adoption of the UID will only ensure that the uniqueness and singularity of each resident is established and authenticated, thereby promoting equitable access to social services.

The adoption of the UID during authentication will also have a direct correlation with subsequent enrolment. Greater enrolment comes from the value a resident derives from the UID, which in turn depends on the rate of adoption. There is a positive cycle here, created from the relationship between adoption and enrolment – the greater the adoption, the faster the enrolment and vice versa. The twin approaches of enrolment and adoption will result in greater influence and traction for the UID among residents in the country, and establish the UIDAI as the only genuine identity authenticator in India.

4.2 Types of authentication

There are multiple forms of authentication that the UID authority can offer. Certain types of authentication would have low to medium assurance if there is the possibility that the card is forged. Here we summarize the main forms of authentication, depending on the situation and equipment available.

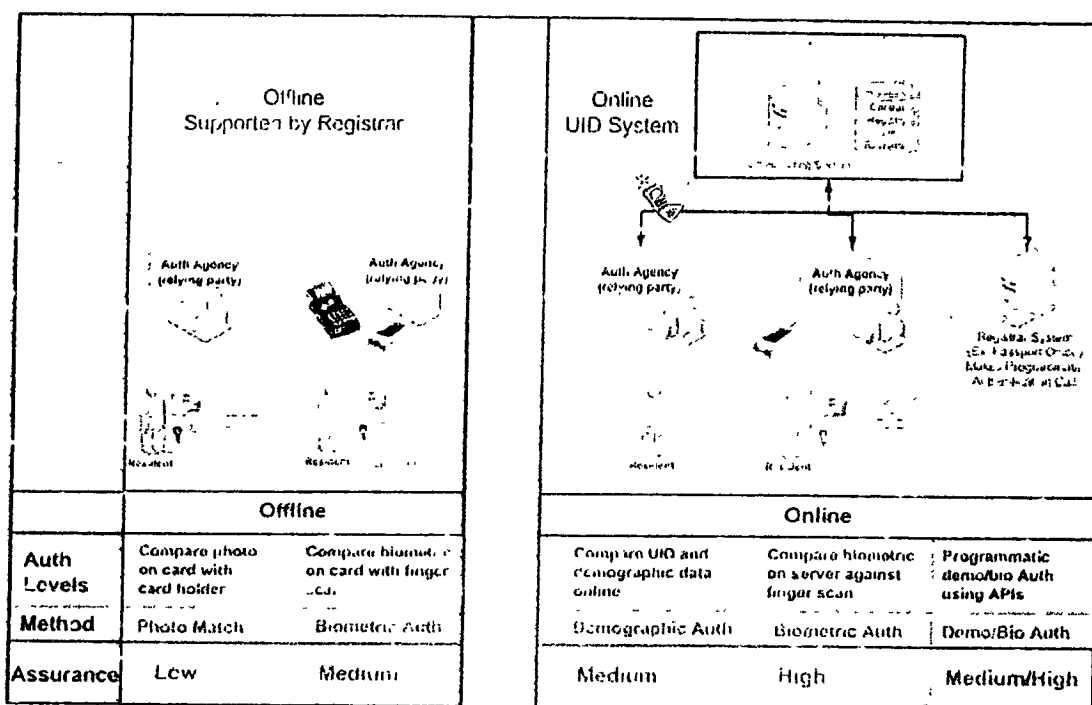
Online authentication is supported by the UID system. This can include

- 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 here is medium.
- Online biometric 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 in this case is high.
- Online demographic/biometric authentication with API where the Registrar's backend system makes a programmatic call to the authentication APIs exposed by the UID system to perform authentication. The assurance level here may be medium-high depending on whether the check used demographic or biometric inputs.

Offline authentication may be supported by the Registrar, and does not use the authenticating service provided by the UIDAI. This may come in two forms:

- Photo match authentication where the photo on the card is compared with the cardholder. This is the most basic form of authentication. The assurance level here is low.

- Offline biometric authentication compares the scanned fingerprint of the cardholder to the biometric stored on the Registrar-issued card. The assurance level here is medium.



4.3 Authentication and the UIDAI revenue model

The ability of the UIDAI to offer agencies across the country strong, reliable authentication is the key to its sustainability. The UIDAI will offer resident authentication services for a fee to governments and private sector firms.

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

Basic identity confirmation

Basic identity confirmation from the UIDAI would be free. In this transaction, the authenticator will provide the UID number, name and one other parameter such as date of birth of the person, and the central database will confirm the identity as a 'Yes' or 'No' response.

This type of transaction will be carried out in large numbers and will need quick response times.

Chargeable authentication services can be of two types:

Address verification

For security purposes, government agencies as well as private sector firms require address proof

from Indian residents before providing them with benefits and services. However, agencies often complain of the difficulty of address verification "you try to verify an address in India, and you enter a labyrinth". 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.

The address authentication service the UIDAI will offer these entities would consequently be a valuable one. In the proposed transaction with the 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.

Biometrics confirmation

Services such as issuing a credit card or granting a loan need the confirmation of the resident's identity. This process for the resident involves the submission of photographs and other documentation confirming their identity. In the proposed transaction with the UID Authority, the agency can send the scanned photograph or fingerprint (based on the security level required) together with other demographic details to confirm the identity of the person.

Revenue projections from authentication services

The following revenue model for the UIDAI is an illustrative one. It has been designed while keeping in mind the value the agency requesting authentication would derive from the service. The table below summarizes the kind of transaction, potential user agencies and the proposed transaction fee. Government agencies could be provided these services from the UIDAI at a subsidized rate.

| Sl. | Transaction Type | Transaction Fee | Potential User Agencies |
|-----|-------------------------|-----------------|------------------------------------|
| 1 | Basic ID Confirmation | Free | Airlines during passenger check-in |
| 2 | Address Verification | Rs. 5 | Banks for account opening |
| 3 | Biometrics Confirmation | Rs. 10 | Credit cards issue process |

The authentication service from the UIDAI can begin after the initial bulk on-boarding of Registrars. The revenue estimates for the UIDAI below are based on the current expenditure of various agencies on KYR processes, which would be replaced by the Authority's authentication services. It also takes into account expected growth in demand for mobile connections, bank accounts, etc.

| UID Revenue Projection (Steady State Estimates) | Transaction Type | |
|--|------------------|------------|
| | Address | Biometrics |
| New Mobile Connections | 19.59 | - |
| PAN Cards | - | 1.20 |
| Gas Connections by PSU | - | 1.50 |
| Passports | 0.06 | - |
| LIC New Policies | - | 10.16 |
| Credit Cards | 0.79 | - |
| Bank Accounts | 11.55 | - |
| Airline Check-in | - | - |
| Projected Total Transactions | 31.91 | 12.86 |
| Proposed Transaction Rate | 5 | 10 |
| Transaction Revenue | 159.55 | 128.60 |
| Estimated total annual revenue at steady state (Rs. Crores) | | 288.15 |

5

Legal Framework

The Constitution of India, through the Directive Principles of State Policy⁵ mandates that the state shall strive to minimize inequalities of income and endeavor to eliminate inequalities in status amongst individuals. The objective of the UIDAI is to solve the key problem of identity that individuals face and enable better and efficient delivery of services to the poor and marginalized so as to eliminate inequalities of income and status. 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 Unique Identification Authority of India (UIDAI) will be set up as a statutory body by an Act of Parliament. The UIDAI will be authorized:

- o To collect the following identity information from any person voluntarily seeking a unique identity number:
 - Name
 - Date of Birth
 - Gender
 - Father's name and UID number
 - Mother's name and UID number
 - Address
 - All ten finger prints, photograph and both iris scans

The law will contain a prescription against collecting any other information than the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters, and for the facilitation of analysis of the data for anyone or to engage in profiling or any similar activity.

- o To issue a unique identity number to the person who has provided the necessary information and fulfilled the requirements as laid down in rules prescribed by the UIDAI.

Art. 38 ⁵(1) The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life

(2) The State shall, in particular, strive to minimise the inequalities in income, and endeavour to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations.

- o To verify the identity of any person at the time of the provision of information, the issuance of a unique identity number or at any other time per the UIDAI database or other possible means, as laid down in rules prescribed by the UIDAI.
- o 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. The information on the database will be used only to authenticate identity.
- o 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.
- o To permit the appointment of Registrars in accordance with criteria laid down by the UIDAI to enrol people that seek unique identity numbers directly or indirectly through enrolling agencies.
- o To allow for the appointment of other service providers in accordance with criteria laid down by the UIDAI, as the UIDAI may deem fit to further its objectives and to ensure efficiency.
- o To call for information and records, conduct inspections, inquiries and audit of the CIDR, Registrars, enrolling agencies and service providers..
- o To enter into all necessary contracts and arrangements in order to fulfill the objectives of the UIDAI.
- o To set up mechanisms for grievance redressal for the public
- o To set up a monitoring framework to improve implementation, create safeguards as required and study the impact of the UID
- o 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

- o 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
- o Penal provisions against persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for breach of certain key sections of the legislation – including the specific prohibitions on profiling, the disclosure of information and maintenance of confidentiality etc.
- o 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. In this context, there will be no liability on the part of the UIDAI or persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for providing a unique identity number to a person who intentionally or fraudulently obtains such number.

Protecting privacy and confidentiality

The information that the UIDAI is seeking is already available with several agencies (public and private) in the country, the additional information being sought by the UIDAI are the finger prints and iris scans. However, the UIDAI recognizes that the right of privacy must be protected, and that people are sensitive to the idea of giving out their personal information, particularly the idea of information being stored in a central database to be used for authentication. 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. Necessary provisions would be in place to address the issues of privacy and confidentiality.

Offences under the UIDAI Act

The UID database will be susceptible to attacks and leaks at various levels. The UIDAI must have enough teeth to be able to address and 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, Registrar or the Enrolling agency
- Disclosure of information violating the protocols set in place by the UIDAI
- Sharing any of the data on the database with anyone.
- Engaging in or facilitating analysis of the data for anyone.
- Engaging in or facilitating profiling of any nature for anyone or providing information for profiling of any nature 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.

6

Data Security and Fraud

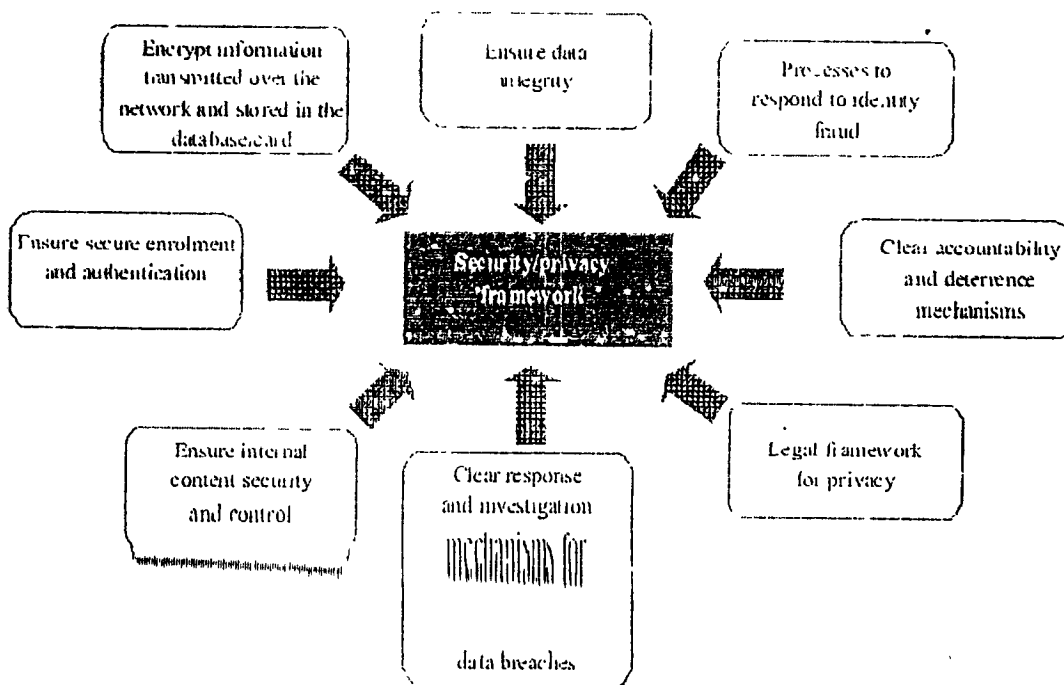
6.1 Protecting personal information of residents

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.

By linking an individual's personal, identifying information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verified and reliable. This means that the resident's identity will possess value, and enable the transfer of money and resources.

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.

In the federated system that the UIDAI envisions, we must consequently have processes in place to ensure a fair level of data security.



6.2 Fraud scenarios

The Authority will concern itself only with identity fraud, which is distinct from document fraud. Document fraud – the use of counterfeited/misleading documents to enter incorrect personal information – will be the responsibility of the Registrar enrolling the resident. The Authority will have clear response mechanisms in place for identity fraud, where an individual deliberately impersonates someone else, either real or fictitious.

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. However, the person will have to exist under this name across systems, in the lifetime of his/her interaction with the government, private agencies and service providers. Such instances are therefore, likely to be rare.

Some of the potential fraud scenarios are:

| Scenario | Response |
|---|---|
| Person applies for a UID number and presents wrong information under their name. | The verification process returns application to the applicant and presents the reasons for not issuing number. |
| Person applies to get a second card in another name. | Application returned, with reason provided. If person's name was fraudulent the first time, he has the option of applying to change his demographic fields. If this fraud is attempted again, person is added to watch list/legal action. |
| Person appears as himself, and applies for a second UID number. | Application returned, with reason provided. If attempted more than three times person added to watch list. |
| Person appears as another existing person, registering the second person's information under his fingerprint. | The victim can report identity theft to the UIDAI's grievance office. The UIDAI will undertake an investigation, and take appropriate action if theft is confirmed. |
| Impersonation of a deceased individual, with fake supporting documents. | If the applicant passes the verification process, then he may be able to take on the stolen identity. However, he will not be able to change his demographic fields over his lifetime without due process. |
| De-duplication works incorrectly and returns false positive for a new UID applicant. | Person can request check against face biometrics as well as re-verification by Registrar. |

7

Technology architecture of the UIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. The architecture has been structured to ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security.

7.1 System architecture

The Central ID Data Repository will be the central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's UID as the key.



The key technology components of the UID system are

- **The UID Server**, which provides the enrolment and the authentication service. These services will be available over the network for the various Registrars and their authenticating agencies to use. The backend servers need to be architected for the high

demands of the 1:N biometric de-duplication as well as the large peak loads from authentication requests.

- **The Biometric sub-system** is central to the UID system for enrolling as well as authenticating residents. It is likely that a multi-modal biometric solution will be used to achieve a high level of assurance. The 1:N de-duplication envisioned will be by far the most computing-intensive operation of the UID system. Innovative techniques of hashing, indexing, distributed processing, and in-memory databases using multiple-biometric-modes need to be employed to get acceptable performance.
- **The Enrolment client application** will capture and validate demographic and biometric data. This client needs to work in an offline mode in the village setting when there is no internet connectivity, and upload batch files to the server for processing. Alternatively the batch files can be physically transported to the CIDR for uploading. The client application will be deployed on a standard enrolment workstation.
- **The Network** is a critical aspect of the system, since all UID enrolment and authentication services will be available online. UID services could work over secure WAN networks, the vanilla internet or over mobile SMS channels. It could also potentially work over existing networks such as credit-card POS (point-of-service) devices.
- **The Security design** secures all the above components from logical/physical attack. This includes.
 - Server Security - firewall, intrusion prevention and detection systems (IPS, IDS)
 - Network, Client Security - Encryption, PKI etc
- **The Administration system** will help administer the UIDAI's operations. This includes
 - Account setup -- creation/modification of Registrar, enrolling and authenticating agency accounts
 - Role based access control - Assign rights over UID resources based on role.
 - Audit trailing - track every access to the UID system.
 - Fraud detection - detect identity theft and cyber crimes using audit trails
 - Reporting and Analytics - Visual decision support tools - GIS, Charting etc.

8

Project Execution

One of the unique challenges in executing the UID project is its scale. Due to the size of India's population, the UIDAI is undertaking what is perhaps the largest governance-related exercise in the world. We must ensure that all aspects of the project – enrolment, de-duplication, and authentication – function effectively even as the number of records approaches a billion.

8.1 Addressing challenges of scale

The UIDAI can expect its enrolment run-rate to have a peak load of one million enrolments per day in the very first year of operation. Every sub-system and component of the UID system will need to scale quickly and significantly. This will include:

- 1) The ability to onboard Registrars from different sectors and handle their constituencies of residents.
- 2) The legal framework of contracts needs to support the variety and spread of stakeholders as their numbers grow exponentially across the country.
- 3) The biometric de-duplication algorithm needs to scale towards checking a fingerprint against every one of 1.2 billion people to ensure uniqueness.
- 4) The authenticating service, which may be used by tens of thousands of points across the country, needs to scale to handle hundreds of thousands of transactions per second.

9

Project Risk

The UID project does face certain risks in its implementation, which have to be addressed through its architecture and the design of its incentives. 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 the poor) the number will not be successful in the long term. To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies and service providers.
- 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 risks in biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.
- 5) **Technology risks:** Technology is a key part of the UID program, and this is the first time in the world that storage, authentication and de-duplication of biometrics are being attempted on this scale. The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.
- 6) **Privacy and security risks:** The UIDAI will have to ensure that resident data is not shared or compromised.
- 7) **Sustainability risks:** The economic model for the UIDAI will have to be designed to be sustainable in the long-term, and ensure that the project can adhere to the standards mandated by the Authority.

10

UID-enabled micro-payment architecture

This section discusses one of the potential applications of the UID – the use of the number in driving financial inclusion, and in enabling a micropayments solution that the poor can use to access financial services.

While the demand for financial inclusion has gained urgency over the last few years, initiatives in India to expand financial infrastructure date back several decades, since the building of rural cooperative credit banks in the 1950s, and the spread of bank networks in the 1970s and 1980s. These initiatives have paid off over the years — India's bank branches are well-networked, particularly across urban India.

But despite these efforts, access to finance has remained scarce in rural India, and for the poorest residents in the country. Today, the proportion of rural residents who lack access to bank accounts remains at 40%, and this rises to over three-fifths of the population in the east and north-east of India.

This exclusion is unfortunate. Economic opportunity is after all, intertwined with financial access. Such financial access is especially valuable for the poor — it offers a cushion to a group whose incomes are often volatile and small. It gives them opportunities to build savings, insure themselves against income shocks and make investments. Such savings and insurance protect the poor against potentially ruinous events — illness, loss of employment, droughts, and crop failures. However due to the lack of access to financial services, many of the Indian poor face difficulties in accumulating savings.

To mitigate the lack of financial access in India, the RBI has focused on improving the reach of financial services in new and innovative ways — through no-frills accounts, the liberalization of banking and ATM policies, and branchless banking with business correspondents² (BC), which enables local intermediaries such as self-help groups, post offices and kirana stores to provide banking services. These efforts have also included the promotion of core-banking solutions in regional rural banks; and the incorporation of the National Payment Corporation of India (NPCI) as an apex switch, for payments and settlements.

In recent years, ATM and core banking, as well as greater mobile connectivity have also become two powerful engines of financial access. Mobile phones in particular present an enormous opportunity in spreading financial services across India. These technologies have reduced the need for banks to be physically close to their customers, and banks have been consequently able to experiment with providing services through online as well as mobile banking. These options, in addition to ATMs, have made banking accessible and affordable for many urban non-poor residents across the country.

With the poor however, banks face a fundamental challenge that limits the success of these technologies and recent banking innovations. The lack of clear identity documentation for the poor creates substantial difficulties in establishing their identity to banks. This has limited the extent to which we can leverage online and mobile banking to reach these communities.

Besides challenges in access and identity, a third limitation has been the cost of providing banking services for the poor. The poor have unique preferences when it comes to withdrawing money and making deposits — they prefer to do large numbers of small transactions, in 'micropayments' of say, Rs.10 rather than Rs.100. Banks discourage such payments, as transaction costs under this model would be too high to bear. The Unique Identification number (UID), which identifies individuals uniquely on the basis of their demographic information and biometrics, gives individuals the means to clearly establish their identity to public and private agencies across the country. It also creates an opportunity to address the existing limitations in financial inclusion. The UID, once it's linked to a bank account, can help poor residents easily establish their identity to banking institutions. As a result, the UID enables banking institutions to bring together the infrastructure that now exists in order to build an accessible, low-cost micropayments model.

Since the UID enables remote authentication of identity, it empowers the poor in making electronic transactions in small, micro-amounts, remotely and at low-cost, through BC networks connected by mobile phones. The model would thus be accessible and affordable across the country. Such a UID-enabled micropayments approach can bring about universal financial access for the poor — they would be able to access their accounts on the move, wherever they are, through any mobile phone, from any BC or bank. The UID-enabled bank account can thus be a global address for residents, similar to an email id or a mobile phone number.

Over the last few years, we have seen critical reforms implemented towards creating a payments solution for the poor. The UID number helps integrate these reforms and leverage the technology already in place into an effective micropayments solution. This can bring low-cost access to financial services to everyone, a short distance from their homes.

10.1 Features of UID-enabled micropayments

UID KYR sufficient for KYC: Banks in India are required to follow customer identification procedures while opening new accounts, to reduce the risk of fraud and money laundering. The strong authentication that the UID offers, combined with its KYR standards, could remove the need for such individual KYC by banking institutions for basic, no-frills accounts. It will thus vastly reduce the documentation the poor are required to produce for a bank account, and significantly bring down KYC costs for banks.

Electronic transactions: The UID's authentication processes will allow banking institutions to verify poor residents both in person and remotely. Rural residents will be able to transact electronically with each other as well as with individuals and firms outside the village, reducing their dependence on cash.

Ubiquitous BC network and BC choice: The UID's clear authentication and verification processes will allow banking institutions to network with village-based BCs such as self-help groups, post offices and kirana stores. Customers will be able to withdraw money and make deposits at the local BC. Multiple BCs at the local level will also give customers a choice of BCs. This would make customers, particularly in villages, less vulnerable to local power structures, and lower the risk of being exploited by BCs.

A high-volume, low-cost revenue approach: The UID will mitigate the high customer acquisition costs, high transaction costs and fixed IT costs that we now face in bringing bank accounts to the poor.

No-frills accounts that can be provided and accessed at low cost through local BCs, with electronic cash transfers, would encourage large numbers of small transactions across these accounts, and make these accounts an important source of revenue for banks.

10.2 Benefits

For residents: The UID-enabled Bank Account (UEBA) will bring financial access and affordability to millions of residents who are presently excluded from formal financial systems. A UID-enabled bank account will also help residents make cheaper, faster electronic transactions and remittances in the form of micropayments. The solution will enable universal access to their account from any bank or BC, and through any mobile device, enabling residents to access payments on the move. Regular, affordable access to banking services would also give the poor a means of keeping their money safe — a convenience that has long been available to the middle class would now be accessible to the rural and urban poor.

For the government: Large-scale financial inclusion can pave the way for electronic benefit transfers (EBTs) for residents. Central and state governments will be able to eliminate the identity-related fraud that exists within its public programs with such transfers going into UID-enabled bank accounts. The bulk of the informal cash economy across rural India, and remittances between urban and rural India will also become part of the formal banking system, with traceable and accountable money flows. This will ensure compliance with Anti-Money Laundering laws and Financial Action Task Force standards. The government will gain these benefits without having to overhaul governance systems — the micropayments approach won't require governments to change decision-making processes across the central, state and local level.

For banking institutions: The use of the central payments switch to move cash electronically at the last mile will dramatically cut down on cash handling and transaction costs for banking institutions. The cost of customer acquisition would also be significantly reduced, as a resident with a UID would require no further identification to get a UID-enabled bank account.

A low-cost micropayment approach will make the large volume of micropayments, remittances and government transfers to UID-enabled bank accounts important sources of revenue for banking institutions. Through the BC network, banks would be able to access customers through

the large distribution channels in the country — including the mobile prepaid network, post office network and FMCG retailers. In addition, BCs would see increased revenues from larger numbers of micro-transactions.

10.3 Conclusion

Over the last decade, we have seen a transformation in financial access for residents across the country — the reforms that encouraged the expansion of ATM, internet and mobile banking have made financial access affordable and accessible for large numbers of residents

The transformation however, has been most significant for India's urban, non-poor residents. These policies have not addressed the unique challenges the poor face in financial access, and they consequently, remain at the periphery when it comes to effective access to finance.

The UID-enabled micropayments solution is just one of the many developmental applications that the UID number can enable. It is also a critically important application, which can help address India's financial divide. Linking the UID number to a universal, accessible, and affordable micropayments model can transform the access the poor have to banking services in the country.

UID-enabled micropayments can be a stepping stone to creating economic opportunities for residents across the country, regardless of where they live. The financial inclusion that it makes possible will be critical to improving access for the poor to resources and skills. As we move towards an open access society, it is this soft infrastructure — connectivity, financial inclusion, and identity — that will ultimately, empower the individual in India.

True Copy

FF

Adv

Exh - 'D'

16/10/12

116

UID for Dummies

Simi Chacko and Pratiksha Khanduri*

August 2011

Released on Kafila on 12 September 2011

Introduction

A. UID: The Basics

B. The Enrolment Process

C. Benefits of UID

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

E. UID and Other Databases

F. Similar Initiatives across the World

Endnote

References

Appendix 1: Valid Identification Documents

Appendix 2: ID Systems and Debates across the World

Notes

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

INTRODUCTION

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

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

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

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

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

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

A. UID: The Basics

Q. 1. What is UID?

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

Q. 2. What about UIDAI?

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

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

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

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

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

According to the UIDAI's "Strategy Overview" document, in India "inability to prove one's identity is one of the biggest barriers preventing the poor from accessing benefits and

subsidies." The document goes on to state "But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence. As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual."⁶

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

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

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

Q. 5. What is "Aadhaar"?

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

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

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

Q. 7. Who is in charge of UIDAI?

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

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

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

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

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

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

Late last year, at a public meeting, Mr. Nilekani stated that the per person enrolment cost is approximately Rs 100.¹¹ "It costs the Unique Identification Authority of India (UIDAI) Rs.100 to generate each *aadhaar* number, which will help address the challenges of inclusion," said Nilekani. Even this is an incomplete answer, because several other agencies are also incurring a cost to enrol each person. Because of the way the system of issuing numbers is set up (see below), there is no transparent way to calculate the cost of this project.

According to the Budget documents, Rs 100 crores was approved in 2009-2010 to fund the agency for its first year of existence. This shot up to Rs 1,900 crores in 2010-11. According

to columnist Praful Bidwai, the Planning Commission is allocating Rs 35,000-45,000 crores over the next five years - to cover only half the population

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

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

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

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

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

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

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

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

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

122
111

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

B. The Enrolment Process

Q. 13. Who will issue the UID number?

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

Q. 14. Who is a "Registrar"?

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

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

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

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

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

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

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

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

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

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

Q.17. How does enrolment proceed?

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

De-duplication will be done by the UIDAI, using the biometrics, to make sure that no-one gets two UID numbers. The UIDAI will also issue the UID number to persons enrolled by Registrars. If any of the personal details (e.g. name and address) recorded at the time of

enrolment change, it is the responsibility of the concerned person to alert UIDAI so that the database can be updated – more on this below.

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

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

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

C. Benefits of UID

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

UID is supposed to act as a general identification facility. "Once residents enrol, they can use the number multiple times – they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on"¹⁷ How useful this "facility" is (and whether it is itself hassle-free) remains to be seen. Aside from this, it is claimed that the UID project is a powerful tool to fight corruption in welfare programmes, enhance inclusiveness in government schemes, and so on. Tall claims have been made, e.g., "the project possesses the power to eliminate financial exclusion, enhance accessibility, and uplift living standards for the majority poor."¹⁸ Some of the specific areas where the benefits of UID are supposed to flow are the National Rural Employment Guarantee Act (NREGA), the Public Distribution System (PDS), public health, financial inclusion, etc. How this is supposed to happen is explained in a series of concept notes posted on the UIDAI website. Three of these concept notes are critically discussed below. The intention is not to say that UID is necessarily useless, but to debunk exaggerated claims and point out that the real benefits are yet to be clearly identified.

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

*UID and NREGA: Claims and clarifications**

Unsuspecting readers of the UIDAI's concept note on "UID and NREGA" may be bowled over by the power of Aadhaar.²⁰ However, a closer look suggests that scepticism is in order.

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

126

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

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

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

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

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

Disruptive potential: Last but not least, UID could easily disrupt NREGA's fragile processes. The UIDAI plans to involve "service providers" who will enrol individuals for

UID. Later, they will be involved in authentication of workers at worksites. The result of such changes will be drastic for NREGA. Payments will come to a halt if workers are still waiting for their Aadhar number. And "service providers" are all set to invade NREGA, outside the framework of the Act, without any safeguards.

Because of this potentially disruptive role of UID in NREGA, nearly 200 scholars and activists signed and circulated a petition called "Keep UID Out of NREGA!" in December 2010.²³ The concerns raised in that petition are yet to be answered.

Will UID Fix the PDS?

Similar reservations apply to the UIDAI's concept note on "UID and PDS System".²⁴ Again, tall claims are made without an adequate understanding of how the PDS works.

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

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

The next question then is, how large is the problem of "ghost" or "duplicate" cards. That question is not easy to answer. It is not clear how large the problem of duplicate or bogus BPL cards actually is. If the recent example of Tamil Nadu weeding out bogus cards is any evidence, then it is only 2% (Planning Commission, 2004). Chhattisgarh tried to achieve de-duplication by computerizing the database of ration card holders and distributing ration cards

with holograms, without relying on UID. Eight per cent of cards were found to be "duplicate"

Further, the elimination of ghost and duplicate cards requires that UID enrolment be compulsory and universal. This is best explained by Nandan Nilekani himself (in an interview to Outlook Business in October 2010): "You can't make it mandatory in the first instance. Let's say a particular state decides to issue fresh ration cards from 1 May 2011. Now, they may decide to have Aadhaar numbers on all these cards. For some time, in parallel there will be the earlier cardholders who will not have Aadhaar. We can't completely eliminate duplication. But over time, as Aadhaar numbers in ration cards become nearly universal, they can then say 'from now onwards, only Aadhaar-based ration cards will be accepted'. At which point, duplication will cease to exist."

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

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

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

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

129

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

UID and Public Health

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

Against this background, the UIDAI shrewdly identified public health as a "killer application" (sic) for UID. As the UIDAI's concept note on "UID and Public Health" states: "Existing data bases would probably still leave a large percentage of the population uncovered. Therefore every citizen must have a strong incentive or a "killer application" to go and get herself a UID, which one could think of as a demand side pull. The demand and pull for this needs to be created *de novo* or fostered on existing platforms by the respective ministries. Helping various ministries visualise key applications that leverage existing government entitlement schemes such as the NREGA and PDS will (1) get their buy-in into the project (2) help them roll out mechanisms that generate the demand pull and (3) can inform a flexible and future-proof design for the UID database. It will also build excitement and material support from the ministries for the UID project even as it gets off the ground."²⁷ The game plan could hardly be more explicit.

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

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

He asserts that UID is not devised to deal with the public health challenges of our country. "On the contrary, given that many diseases continue to bear a stigma in this country, the UID scheme has the unique potential of increasing stigma by breaching the anonymity of health data collected. It thus violates the heart of the medical encounter, namely confidentiality. By

making this information potentially available to employers and insurance companies, the scheme bodes further gross violations of health rights "

Referring to the NGO reports about the Delhi government's "Mission Convergence" scheme, under which biometric health insurance cards were issued to slum dwellers by which they could avail free treatment, Rao holds that there have been a lot of complaints about malfunctioning fingerprint readers, despite multiple swipes. He advises the Health Ministry to hold back on their support for UID until a conclusive study of the costs and risks of this project is undertaken.

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

Q. 20. What are biometrics?

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

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

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

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

A recent NASSCOM document, prepared by Dr. Kamlesh Bajaj, points out that since the UID database has to be accessible over networks in real time, it involves major operational and security risks - as with any such applications.³⁰ If networks fail or become unavailable, the entire identification system may collapse. Biometric and other data may become a target

for hackers and other malicious entities "Such a system is also prone to functional creep (secondary uses) and insider abuse. There is also a significant risk of transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection"

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

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

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

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

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

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

Biometrics: Reliable or Fallible?

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

Here's why biometric systems have a shaky base:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q. 24. Is there a redressal mechanism?

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

E. UID and Other Databases

Q. 25. What is NATGRID?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Little is known about how the government plans to integrate UID with NPR. In the village of Tembali, both were meant to work together in capturing biometrics. The Census Office (also known as the Registrar General of India) has been given the authority to collect the biometric data through an Act of Parliament. But the information recorded by the private enrolment agency working for UIDAI is different from the details captured by the census enumerators. Unique identity numbers were meant to be issued by the agency based on the information recorded for NPR. This meant that while every Indian resident would have an NPR card and a UID number, the enrolment was meant to be carried out by the Census office³⁹.

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

13.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q. 30. More than meets the eye?

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

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

Department of Defense and has contracts with nearly every intelligence agency in the government. L-1 was rejected by US government agencies on grounds of low quality of its biometric cards. In June 2010, a support contract unit of L-3 Communications Corp said it was de-listed from providing service to any federal agencies in the US. The support contract unit was providing aircraft maintenance and logistic support to the US Air Force. The unit allegedly used government computer networks to collect data to promote its own business. In September 2010, the company received US\$ 24 million for the project from the UIDAI. The company has already shipped some units of the Agile TP fingerprint slap devices and mobile iris cameras. In a Forward Looking Statement the company said it hopes to complete the remainder of the shipment by March 2011.⁴⁹

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

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

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

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

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

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

(4)

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

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

The use of biometrics in consumer ID applications worldwide are projected to grow at a Compound Annual Growth Rate (CAGR) of around 27% between 2010 and 2012.⁵⁴ With advancements in sensor technology and algorithms, biometrics seem to have become a choice for the financial services industry as well.

F. Similar Initiatives across the World

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

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

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

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

142

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

11

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

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

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

END NOTE

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

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

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

References

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

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

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

"UIDAI rolls out 10 Lakh 'Aadhaar' Numbers", Times of India, January 13th, 2011
(http://articles.timesofindia.indiatimes.com/2011-01-13/india/28370904_1_aadhaar-enrolments-unique-identification-number)

Additional Links

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

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

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

Appendix 1 Valid Identification Documents

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

Documents Containing Name and Photo

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

Documents Containing Name and Address

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

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

Proof of Date of Birth Documents

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

Appendix 2 ID Systems and Debates across the World

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

European Countries

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

France

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

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

Germany

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

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

United Kingdom

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

Bosnia

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

United States of America

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

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

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

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

150

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

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

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

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

Canada

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

Pakistan

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

Malaysia

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

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

Japan

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

Taiwan

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

People's Republic of China

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

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

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

Australia

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

West Asia

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

- ¹ Sriniwasaraju, Sugata, "Biometry Is Watching", Outlook, 17th May, 2010 (<http://www.outlookindia.com/article.aspx?265326>)
- ² Narendra Kaushik (2011), "Cards to Nowhere", *Inclusion*, April-June 2011
- ³ Gupta, Vishv, "What the UID project will not do", Tehelka, 2nd June, 2011 (http://www.tehelka.com/story_main49.asp?filename=WS020611UIDproject.asp)
- 4 UIDAI, "UIDAI Strategy Overview: Creating a unique identity number for every resident in India", available at http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overview-001.pdf
- 5 PRS India, "The National Identification Authority of India Bill, 2010", available at <http://prsindia.org/upload/media/UID/The%20National%20Identification%20Authority%20of%20India%20Bill,%202010.pdf>
- 6 UIDAI, "UIDAI Strategy Overview: Creating a unique identity number for every resident in India", available at http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overview-001.pdf
- 7 Mittal, Tusha, "Falling Between the Bar Codes", Tehelka, August 22nd, 2009. (http://www.tehelka.com/story_main42.asp?filename=N-220809falling_between.asp)
- 8 Moneylife.in, "No card, only a number despite Rs. 45,000 crore being spent on the UID project", available at <http://www.moneylife.in/article/8/6920.html>
- 9 See <https://portal.uidai.gov.in/uidwebportal/dashboard.do>
- 10 Bidwa, Pratu, "Why Indians Should Fear the UID", Rediff News, October 12th, 2010 <http://www.rediff.com/news/column/column-why-indians-should-fear-the-uid/20101012.htm>
- 11 Editor's Guild of India's Annual Rajinder Mahur Memorial Lecture attended by writers of this primer (<http://expressbuzz.com/nation/each-unique-id-number-costs-rs100-nilekani/227888.html>)
- 12 Dreze, Jean, Unique Facility or Recipe for Trouble, The Hindu, November 25th, 2010
- 13 Sanyal, Kaushiki and Kumar, Rohit (2011), "The National Identification Authority of India Bill (2010)", PRS Legislative Research, June 2nd, 2011 (<http://indiahyers.wordpress.com/2011/06/19/the-national-identification-authority-of-india-bill-2010/>)
- 14 Justice.gov, Overview of the Privacy Act of 1974, 2010 Edition, (<http://www.justice.gov/opcl/1974ssn.htm>)
- 15 UIDAI, "Registrar FAQs: Summary of responses to Questions Frequently Asked by Registrars", available at <http://uidai.gov.in/images/FrontPageUpdates/ROB/A2%20Registrar%20FAQs.pdf>
- 16 Sethi, Nitin, "NGO's shelter shut after it pointed out UID flaws", Times of India, 4th July 2011, http://articles.timesofindia.indiatimes.com/2011-07-04/india/29735661_1_uid-enrollment-ngo-igss
- 17 UIDAI, "UIDAI Strategy Overview: Creating a unique identity number for every resident in India" available at http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overview-001.pdf
- 18 UIDAI, "UID and NREGA" (http://uidai.gov.in/UID_PDF/Working_Papers/UIDandNREGA.pdf),
- 19 Agarwal, Surabhi, "UID Puts Revenue Stream on Hold", Livemint, 16th February, 2011 (<http://www.livemint.com/2011/02/16010317/UID-puts-revenue-stream-on-hold.html?atype=tp>)
- 20 UIDAI, "UID and NREGA" (http://uidai.gov.in/images/FrontPageUpdates/uid_and_nregga.pdf).
- 21 On the issue of corruption and the transition to bank and post office payment of NREGA wages, see Siddharth and Vanaik (2008), Dreze and Kherna (2008), and Adhikari and Bhatia (2010).
- 22 "UID Project (Aadhar) Issue Overview",
- 23 See <http://www.sacw.net/article1722.html>.
- 24 UIDAI, "UID and PDS System", available at http://uidai.gov.in/images/FrontPageUpdates/uid_and_pds.pdf

- 25 See various documents posted on the website of the right to food campaign (www.righttofoodindia.org), also the recent "open letter" to the Prime Minister on this subject, based on a survey of the PDS in nine states (<http://www.sacw.net/article2207.html>)
- 26 Tha Indian News, "Lacking Healthcare, A Million Indians Die Every Year", 2nd February, 2009 (http://www.thaindian.com/newsportal/world-news/lacking-healthcare-a-million-indians-die-every-year-oxford-university_100150164.html)
- 27 UIDAI, "UID and Public Health", (http://uidai.gov.in/UID_PDF/Working_Papers/UIDandPublicHealth.pdf)
- 28 Rao, Mohan, "UID and Public Health: Magic Bullet or Poison Pill", The Asian Age, 24th December, 2010 (<http://www.asianage.com/ideas/uid-public-health-magic-bullet-or-poison-pill-977>)
- 29 Pato and Millette (2010), "Biometric Recognition: Challenges and Opportunities"
- 30 Dr. Kamlesh Bajaj, "Security and Privacy Challenges in the Unique Identification Project," Project RISE (A NASSCOM initiative) 25th March, 2010
- 31 Ton van der Puetter and Jeroen Keuning "Biometrics and Fingerprints", (<http://keuning.com/biometry/>)
- 32 London School of Economics and Political Science (2005), The Identity Project: An assessment of the UK Identity Cards Bill and its Implications (London: London School of Economics and Political Science).
- 33 Also refer to Drèze, Jean (2010), "UID: Unique Facility or Recipe for Trouble?", The Hindu, 25 November (<http://www.hindu.com/2010/11/25/stories/2010112563151300.htm>)
- 34 Kakatkar-Kulkarni, Manasi, "Chidambaram proposes radical restructuring of India's security structure", Foreign Policy Association, December 23rd, 2009 (<http://india.foreignpolicyblogs.com/2009/12/23/chidambaram-proposes-radical-restructuring-of-indias-security-structure/>)
- 35 Pandey, Brijesh, "Natgrid will kick in from May 2011. Is the big brother threat for real?", November 13th, 2010 (http://www.tehelka.com/story_main47.asp?filename=Ne131110Natgrid_will.asp). Also refer to (<http://news.rediff.com/report/2010/feb/06/natgrid-will-track-all-your-spending.htm>)
- 36 Times News Network, "CCS seeks tighter privacy safeguards in NATGRID proposal," Times of India, February 11th, 2010 (<http://timesofindia.indiatimes.com/india/CCS-seeks-tighter-privacy-safeguards-in-NATGRID-proposal/articleshow/5557716.cms#ixzz1B8WSNJ9e>)
- 37 Governance Now, "Fin min says no to Natgrid spying on bank account-holders", 27th September 2010, (<http://www.governancenow.com/news/regular-story/fin-min-says-no-natgrid-spying-bank-account-holders>)
- 38 Hindustan Times, "Cabinet clears creation of National Population Register", 19th March 2010, (<http://www.hindustantimes.com/Cabinet-clears-creation-of-National-Population-Register/Article1-521016.aspx>)
- 39 "Aadhar: Pied Piper of Technology", Inclusion, April- June 2011 (http://www.inclusion.in/index.php?option=com_content&view=article&id=669:cover-story&catid=234:editor)
- 40 Dhoot, Vikas, "Nandan Nilekani's UIDAI and Census' NPR in role overlap for fingerprinting and other biometric data", Economic Times, 11th August 2011 (<http://m.economictimes.com/PDAET/articleshow/9560067.cms>)
- 41 Rahman, Shafi, "Unique ID project hits legal hurdle", India Today, 25th July 2010, (<http://indiatoday.intoday.in/site/story/unique-id-project-hits-legal-hurdle/1/144988.html>)
- 42 Ramanathan, Usha, "Implications of registering, tracking and profiling", The Hindu, 4th April, 2010 (<http://www.thehindu.com/opinion/lead/article388037.ece>)
- 43 Zaba, Christina, "When the eyes don't have it," New Statesman, 30th May, 2010 (<http://www.newstatesman.com/200505300020>). Also refer to <http://nprindia.blogspot.com/search?updated-min=2008-01-01T00:00:00-08:00&updated-max=2009-01-01T00:00:00-08:00&max-results=9>

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

- (http://www.computerworld.com/s/article/print/9204858/Real_ID_alive_and_kicking_report_says), and
(<http://www.govtech.com/security/99354049.html>)

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

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

Also check:

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

True Copy
F.
Adv

Background to the UID

(ACCESSED from the UID Website:

http://uidai.gov.in/index.php?option=com_content&view=article&id=141&Itemid=164#background)

Unique identification project was initially conceived by the Planning Commission as an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

a) The concept of a unique identification was first discussed and worked upon since 2006 when administrative approval for the project –"Unique ID for Below Poverty Line (BPL) families" was given on 03 March 2006 by the Department of Information Technology, Ministry of Communications and Information Technology. This project was to be implemented by the National Informatics Centre (NIC) over a period of 12 months. Subsequently, a Processes Committee to suggest processes for updation, modification, addition and deletion of data fields from the core database to be created under the Unique ID for below BPL project was set up on 03 July 2006. This was set up under the chairmanship of Dr. Arvind Virmani, Principal Adviser, Planning Commission.

b) A "Strategic Vision on the UIDAI Project" was prepared and submitted to this Committee by M/S Wipro Ltd (Consultant for the design phase and program management phase of the Pilot UIDAI project). It envisaged the close linkage that the UIDAI would have to the electoral database. The Committee also appreciated the need of a UIDAI Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the authority and at the same time enable a focused approach to attaining the goals set for the XI Plan. The Seventh Meeting of the Process Committee on 30 August 2007 decided to furnish to the Planning commission a detailed proposal based on the resource model for seeking its "in principle" approval.

c) At the same time, the Registrar General of India was engaged in the creation of the National Population Register and issuance of Multi-purpose National Identity Cards to citizens of India.

d) Therefore, it was decided, with the approval of the Prime Minister, to constitute an empowered group of Ministers (EGoM) to collate the two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number project of the Department of Information Technology. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these. The EGoM was constituted on 04 December 2006.

- The first meeting of the EGoM was held on 27 November 2007. It recognised the need for creating an identity related resident database,

regardless of whether the database is created based on a de-novo collection of individual data or is based on already existing data such as the voter list, there is a crucial and imperative need to identify and establish an institutional mechanism that will "own" the database and will be responsible for its maintenance and updating on an ongoing basis post its creation.

- The second meeting of the EGoM was held on 28 January 2008. It decided on the strategy for the collation of NPR and UIDAI. Inter-alia, the proposal to establish UIDAI Authority under the Planning Commission was approved.

- The third meeting of the EGoM was held on 07 August 2008. The Planning Commission had placed before the EGoM a detailed proposal for setting up UIDAI. The meeting decided that certain issues raised by the members with relation to the UIDAI (Annexure to the EGoM meeting proceedings) would need to be examined by an official level committee. It referred the matter to a Committee of Secretaries to examine and give its recommendations to the EGoM to facilitate a final decision.

- Subsequent to the Committee of Secretaries recommendations, the fourth meeting of the EGoM was held on 04 November 2008. The recommendations of the Committee of Secretaries were presented to the EGoM and the following decisions were taken.

- a) Initially the UIDAI may be notified as an executive authority and investing it with statutory authority could be taken up for consideration later at an appropriate time.

- b) UIDAI may limit its activities to creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.
- c) UIDAI will take its own decision as to how to build the database.
- d) UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.
- e) Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure through the DoE/CCEA.
- f) Approval to the constitution of the State UIDAI Authorities simultaneously with the Central UIDAI with a core team of 3 personnel.
- g) December 2009 was given as the target date for UIDAI to be made available for usage by an initial set of authorized users.
- h) Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed

organizational structure, staff and other requirements.

1.1: Subsequently, on 22 January 2009 the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers considered the proposal submitted by the Department of Information Technology regarding the governance structure and recommended that

a) The notification for constitution of the UIDAI should be issued immediately.

b) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission to be constituted to oversee the work of the authority.

c) A Member, Planning Commission or the Secretary, Planning Commission may also be assigned the task of looking after the work proposed for the Chief UIDAI Commissioner.

d) Core Team to be put in place.

1.2: In pursuance of the Empowered group of Ministers' fourth meeting dated 04 November 2008, the Unique Identification Authority of India was constituted and notified by the Planning Commission on 28 January 2009 as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. The role and responsibilities of the UIDAI was laid down in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UIDAI scheme and shall own and

operate the UIDAI database and be responsible for its updation and maintenance on an ongoing basis.

Top

Prime Minister's Council

Prime Minister's Council on UIDAI Authority - Subsequently, on 02 July 2009, the Government appointed Shri. Nandan M. Nilekani as Chairman of the Unique Identification Authority of India, in the rank and status of a Cabinet Minister for an initial tenure of five years. Mr. Nilekani has joined the UIDAI as its Chairman on 23 July 2009. The Prime Minister's Council of UIDAI Authority of India was set up on 30 July 2009. The Council is to advise the UIDAI on Programme, methodology and implementation to ensure co-ordination between Ministries/Departments, stakeholders and partners. The Council would meet once every quarter. The First Meeting of the Prime Minister's Council of UIDAI Authority took place on 12 August 2009.

The salient decisions in the PMs council were as follows :

Need for legislative framework

Broad Endorsement of the Strategy

Budgetary Support to partners

Setting Biometric and Demographic Standards

UIDAI Structure Contours Approved

Flexibility in Personnel and other issues

Choose, Deploy and Repatriate Officers

Government Accommodation Eligibility

Broad-banding of posts

Hiring of professionals from Market

Setting up of Global Advisory Councils of PIOs

Interns and Sabbatical Global Procurement

Top

Cabinet Committee

The Government of India issued orders constituting the Cabinet Committee on UIDAI Authority on 22 October 2009. It is headed by the Honourable Prime Minister and consists of the Minister of Finance, Minister of Agriculture, Minister of Consumer Affairs, Food and Public Distribution, Minister of Home Affairs, Minister of External Affairs, Minister of Law and Justice, Minister of Communications and Information Technology, Minister of Labour and Employment, Minister of Human Resource Development, Minister of Rural Development and Panchayati Raj, Minister of Housing and Urban Poverty Alleviation and Minister of Tourism. The Deputy Chairman Planning Commission and Chairman UIDAI are special invitees. The functions of the Committee, which is headed by the Honourable PM would be as under :

All issues relating to the Unique identification Authority of India including its organisation, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

Mandates and Objectives

The Unique Identification Authority of India (UIDAI) has been created as an attached office under the Planning Commission. Its role is to develop and implement the necessary institutional, technical and legal infrastructure to issue unique identity numbers to Indian residents.

On 25 June 2009, the Cabinet also created and approved the position of the

Chairperson of the UIDAI, and appointed Mr. Nandan Nilekani as the first Chairperson in the rank and status of a Cabinet Minister. Mr. Ram Sewak Sharma has been appointed the Director General.

Mission and Timeline

Top

The Mission

The role that the Authority envisions is to issue a unique identification number (UIDAI) that can be verified and authenticated in an online, cost-effective manner, which is robust enough to eliminate duplicate and fake identities.

The Timelines

The first UIDAI numbers will be issued over the next 12-18 months counted from August 2009. The first number would be issued between August 2010 to February 2011. Over five years, the Authority plans to issue 600 million UIDs. The numbers will be issued through various 'registrar' agencies across the country.

Top

Organization Details

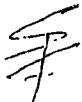
UIDAI was set up as an attached office of the Planning Commission through Notification dated 28.01.09 with a core team of 115 officers and staff. Under the Notification, 3 Posts (DG, DDG and ADG) were sanctioned for Headquarter with 35 UID commissioners in each of the States. It was thereafter decided to have Regional Offices in Bangalore, Chandigarh, Delhi, Hyderabad, Guwahati, Lucknow, Mumbai and Ranchi with their jurisdiction covering specific states across the country. A Technology Centre has been set up in Bangalore. 268 additional posts were created in September 2009. UIDAI at present has a total sanctioned strength of 383

165

officers and subordinate staff.

Headquarter's Organisation: The UIDAI is headquartered in Delhi with Shri Nandan Nilekani as the Chairman and Shri R.S. Sharma as the Director General and Mission Director. In the organizational design, the DG is to be assisted by seven Deputy Director Generals, officers of the level of Joint Secretary, who are in charge of various Wings. One of the DDGs heads the Finance Wing. The DDGs would be supported by 21 ADGs, 15 Deputy Directors, 15 Section Officers and 15 Assistants. The HQ has a total sanctioned strength of 146 number of officers and staff including the Accounts and IT branch. All the officers and staff have been appointed on deputation either under Central Staffing Scheme or through bilateral route. Of the sanctioned strength, 85 are in position at present. Appointments for the remaining vacancies are in process.

True Copy



Adv

Exh-F

1610112 2
Annexure 2

166

(TO BE PUBLISHED IN PART-I, SECTION-2 OF THE GAZETTE OF INDIA)

GOVERNMENT OF INDIA
PLANNING COMMISSION

Yojana Bhawan, Sansad Marg,
New Delhi, 28th January, 2009

NOTIFICATION

No. A-43011/02/2009-Admin.I. In pursuance of Empowered Group of Ministers' fourth meeting, dated 4th November 2008, the Unique Identification Authority of India (UIDAI) is hereby constituted and notified as an attached office under aegis of Planning Commission with following terms of reference and initial core staff composition:-

COMPOSITION:

- 2 UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:

| Post | Level | No. of Posts |
|-------------------------------------|-------------------------------------|--------------|
| UID Authority of India | | |
| Director General & Mission Director | Additional Secretary Govt. of India | 1 |
| Deputy Director General (DDG) | Joint Secretary, Govt. of India | 1 |
| Assistant Director General (ADG) | Director, Govt. of India | 1 |
| Support Staff | | |
| PS | PS | 3 |
| Peon | Peon | 2 |
| Driver | Driver | 2 |
| Total Manpower | | 10 |
| State /UT Units of UIDAI | | |
| State / UT UID Commissioner | Joint Secretary, Govt. of India | 35 |
| Support Staff | | |
| PS | PS | 35 |
| Peon | Peon | 35 |
| Total Manpower | | 105 |
| Grand Total | | 115 |

Role and Responsibilities of UIDAI

- 3 UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and operate UID database and be responsible for its updation and maintenance on an ongoing basis
- 4 Implementation of UID scheme will entail, *inter alia*, following responsibilities being undertaken by UIDAI
- Generate and assign UID to residents
 - Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
 - Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
 - Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism
 - Define usage and applicability of UID for delivery of various services
 - Operate and manage all stages of UID lifecycle
 - Adopt phased approach for implementation of UID specially with reference to approved timelines
 - Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
 - Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
 - Evolve strategy for awareness and communication of UID and its usage
 - Identify new partner / user agencies
 - Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases
 - Frame policies and administrative procedures related to hiring / retention / mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI.
- 5 Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning and budgetary support. Planning commission would provide initial office and IT Infrastructure at central level

168

Annexure 1

6 Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development.

(Signature)
(Dr. Subbar Pant) 28/11/0

Secretary to the Government of India

The General Manager
Govt. of India Press
Faridabad.

Copy to

- 1 Secretary to the President, Rashtrapati Bhavan, New Delhi
- 2 Secretary to the Vice-President, Maulana Azad Road, New Delhi
- 3 Cabinet Secretary, Rashtrapati Bhavan, New Delhi
- 4 Principal Secretary to the Prime Minister, South Block, New Delhi
- 5 Private Secretary to the Deputy Chairman, Planning Commission
- 6 All Ministers/Departments of Govt. of India
- 7 Chief Secretaries of all States/Union Territories
- 8 Secretary General, Rajya Sabha Secretariat, New Delhi
- 9 Secretary General, Lok Sabha Secretariat, New Delhi
- 10 Pr. Adviser (Admn & PC)/AS & FA/Adviser (C & I)/Director (GA)/DS (Admn.)
- 11 Pay & Accounts Officer, Planning Commission
- 12 Drawing & Disbursing Officer, Planning Commission
- 13 Accounts -I Section, Planning Commission.

True Copy

(Signature)
Adv

TO

Exh - 61

16/10/12

16/RTI/2012
3/6/2012

The Public Information Officer

1.69

At 13/10/12

State of Karnataka

Bangalore

Minister, Information & Public

Public Relations

Government of Karnataka

Bangalore

Dear Sir

Subject: On the constitution of the appoint-
ment of members of the

Committee

I am applying for details of the constitution of
the UDAP and the appointment of members for
the UDAP. I am also interested to know the
details of the members of the UDAP. I am
also interested to know the details of the
UDAP. I am also interested to know the
details of the UDAP. I am also interested to
know the details of the UDAP. I am also
interested to know the details of the UDAP.

The details of the members of the UDAP are
attached along with this letter.

I am also enclosing the details of the UDAP
via Draft No. 81E/235711.

Also, as per the provisions of the RTI Act 2005,
please provide the details of the name and desig-
nation of the person appointed to the UDAP.
I respect to your representative and reply to
the enclosed request.

Name of the Applicant: Thana Sampetty and
Signature Subramaniam

170

Address: D-57, 11, 4th floor,

Major Road, Madurai

Post Office: 625 001

Particulars of Information Required: Information
on the constitution and appointment of personnel
in the unit.

- (i) Constitution and appointment of personnel ✓
- (ii) Process by which information is received: current
- (iii) Description of information:
 - a) What was the process followed in the appointment of the members of CHDA?
 - b) Who were the members, elect, after the current champion, nominated for appointment as champion of CHDA?
 - c) What were the criteria qualifications and experience stipulated for the above position?
 - d) How were these criteria decided and by whom?

Information received by post or in person.

171

(iv) whether applicant is BPL. No

Place: Delhi

Date: 27.05.2010

Yashraj (TEISHNA GEMRATY)
27.05.10.

172
F-12013/08/RTI/2010-CPIO / 1469
Government of India
Planning Commission
Unique Identification of India

Jeevan Bharati Building
Third Floor, Tower -II
Connaught Circus, New Delhi- 110 001
Date: 2nd July 2010

Subject: Information under Right to Information Act 2005.

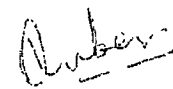
Sir,

Please refer to your letter dated 27th May 2010 received in this office on 3rd June 2010 seeking information under Right to Information Act 2005 on constitution and appointment of personnel in UIDAI.

The decision for appointment of Chairman UIDAI was conveyed by the Cabinet Secretariat. In this connection a copy of Press Release from PIB is enclosed.

If you are not satisfied with the reply of CPIO, UIDAI, you may appeal to Appellate Authority, UIDAI within 30 days from the receipt of this letter. The address and contact number of the Appellate Authority are given below:

Mrs K. Ganga
DDG & Appellate Authority
Unique Identification Authority of India (UIDAI)
Third Floor, Tower -II
Jeevan Bharati Building
Connaught Circus, New Delhi- 110 001
Tel Phone No 2375 2672


(JAYA DUBEY)
ADG & CPIO
Ph No 23752764

To
Trishna Senapaty
D35, IFS CGHS, Mayur Vihar,
Phase -I, New Delhi- 110091

173

GOVERNMENT OF INDIA
PLANNING COMMISSION

Yojana Bhavan, Sansad Marg,
New Delhi 110029, July, 2009.

NOTIFICATION

No A-43011/02/2009-Adm.I (Vol II) In continuation of Notification number A-43011/02/2009-Adm.I dated 28.1.2009 regarding creation of Unique Identification Authority of India (UIDAI) as an Attached Office of the Planning Commission, it is notified that the competent authority has approved the appointment of Shri Nandan Nilekani, Co-Chairman, INFOSYS as Chairperson, Unique Identification Authority of India, in the rank and status of a Cabinet Minister. Shri Nilekani will hold appointment for an initial tenure of five years.

(Anil Malhotra)

Deputy Secretary to the Govt. of India

The General Manager,
Govt of India Press,
Faridabad

Copy to -

1. Shri Nandan Nilekani, CEO, President & MD, Infosys Technologies Ltd., Corporate Headquarters, Plot No. 44 & 97 A, Electronics City, Hosur Road, Bangalore.
2. Secretary to the President, Rashtrapati Bhavan, New Delhi.
3. Secretary to the Vice-President, Maulana Azad Road, New Delhi.
4. P.M.'s Office (Principal Secretary to PM), South Block, New Delhi.
5. P.S. to Deputy Chairman, Planning Commission
6. Cabinet Secretariat (Cabinet Secretary), Rashtrapati Bhavan, New Delhi w.r.t. their note No. 1-1/2009-CS (A) (pt.) dated 01.07.2009.
7. Secretary (Personnel), North Block, New Delhi.
8. Secretary, Planning Commission / Principal Adviser (Admn.), Planning Commission.
9. Director General, UIDAI / Adviser (C&I), Plg Commission
10. All Ministries / Department of Government of India
11. Chief Secretaries of all States / Union Territories of India.
12. Secretary General, Rajya Sabha Secretariat, New Delhi.
13. Secretary General, Lok Sabha Secretariat, New Delhi.
14. Message Section, Rashtrapati Bhavan, New Delhi.
15. Public Section, Ministry of Home Affairs, North Block, New Delhi.
16. Accounts I Section, Planning Commission.
17. Drawing and Disbursing Officer, Planning Commission.
18. Pay & Accounts Office, Planning Commission.
19. Personal File of Shri Nandan Nilekani.
20. Circulated in Yojana Bhavan through e-mail.

17676

2/7/09

to govt.
P.M.

by
Sd/-

Sec. Secy

Adm. Secy

11/07/09

Secy (C&I)

2/7/09

(Anil Malhotra)

Deputy Secretary to the Govt. of India

True copy

Adv

Exh. 17
(610112)
194

BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION

Paul Ohm*

Computer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name for techniques that protect the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated that they can often "reidentify" or "deanonymize" individuals hidden in anonymized data with astonishing ease. By understanding this research, we realize we have made a mistake, labored beneath a fundamental misunderstanding, which has assured us much less privacy than we have assumed. This mistake pervades nearly every information privacy law, regulation, and debate, yet regulators and legal scholars have paid scant attention. We must respond to the surprising failure of anonymization, and this Article provides the tools to do so.

| | |
|---|------|
| INTRODUCTION | 1703 |
| I. ANONYMIZATION AND REIDENTIFICATION | 1706 |
| A. The Past: Robust Anonymization | 1706 |
| 1. Ubiquitous Anonymization | 1707 |
| a. The Anonymization/Reidentification Model | 1707 |

* Associate Professor, University of Colorado Law School. This Article was presented at the Privacy Law Scholars Conference and at conferences and faculty workshops at Harvard's Center for Research and Computer Science and Berkman Center, Princeton's Center for Information Technology Policy, Fordham University Center for Law and Information Policy, University of Washington School of Law, University of Washington's Computer Science & Engineering Department, NYU Information Law Institute, DePaul Center for IP Law and Information Technology, International Association of Privacy Professionals Global Privacy Summit, and the University of Colorado Law School. I thank all participants for their comments.

Thanks in particular to Caspar Bowden, Ramon Caceres, Ryan Calo, Deborah Cannrell, Danielle Citron, Nestor Davidson, Pierre de Vries, Vasant Dhar, Cynthia Dwork, Jed Elia, Ed Felten, Victor Heisler, Susan Friwald, Brett Frischmann, Michael Froeman, Simon Garfinkel, Lauren Gelman, Eric Goldman, James Grimmelmann, Mike Hintze, Chris Hofmann, Chris Hunsington, Jeff Jonas, Jerry Kang, Nancy Kim, Jon Kleinberg, Sarah Krakoff, Tim Lee, William McGeveran, Devon McGraw, Viva Moffat, Tyler Moore, Arvind Narayanan, Helen Nissenbaum, Scott Peppett, Jules Polonetsky, Foster Provost, Joel Reidenberg, Ira Rubinstein, Andrew Schwartz, Ari Schwartz, Vitaly Shmatikov, Chris Soghoian, Dan Solove, Laranyi Sweeney, Peter Swire, Sahil Vadhan, Michael Waggoner, Phil Weiser, Rebecca Wright, Felix Wu, and Michael Zimmer for their comments. This research was supported by a picture research leave grant by the University of Colorado Law School, and for this I thank Dean David Gerches and Associate Dean Dayna Matthew. Finally, I thank my research assistant, Jerry Green.

| | |
|---|------|
| b. The Reasons to Anonymize | 1708 |
| c. Faith in Anonymization | 1710 |
| 2. Anonymization Techniques: The Release-and-Forget Model | 1711 |
| B. The Present and Future: Easy Reidentification | 1716 |
| 1. How Three Anonymized Databases Were Undone | 1717 |
| a. The AOL Data Release | 1717 |
| b. ZIP, Sex, and Birth Date | 1719 |
| c. The Netflix Prize Data Study | 1720 |
| 2. Reidentification Techniques | 1723 |
| a. The Adversary | 1723 |
| b. Outside Information | 1724 |
| c. The Basic Principle Of Crossed Hands and Inner Join | 1725 |
| 3. Responding to Objections | 1727 |
| a. No Harm, No Foul | 1728 |
| b. Examples of Bad Anonymization | 1728 |
| c. The Problem of Public Release | 1729 |
| d. The Myth of the Superuser | 1730 |
| 4. The Intuition Gap | 1731 |
| II. HOW THE FAILURE OF ANONYMIZATION DISRUPTS PRIVACY LAW | 1731 |
| A. The Evolution of Privacy Law | 1732 |
| 1. The Privacy Torts: Compensation for Harm | 1732 |
| 2. Shift to Broad Statutory Privacy: From Harm to Prevention and PII | 1733 |
| 3. How Legislatures Have Used Anonymization to Balance Interests | 1735 |
| a. How HIPAA Used Anonymization to Balance Health Privacy | 1736 |
| b. How the EU Data Protection Directive Used Anonymization to Balance Internet Privacy | 1738 |
| B. How the Failure of Anonymization Disrupts Privacy Law | 1740 |
| C. The End of PII | 1742 |
| 1. Quitting the PII Whack-a-Mole Game | 1742 |
| 2. Abandoning "Anonymize" and "Deidentify" | 1744 |
| III. HALF MEASURES AND FALSE STARTS | 1745 |
| A. Strictly Punish Those Who Harm | 1746 |
| 1. The Accretion Problem | 1746 |
| 2. The Database of Ruin | 1748 |
| 3. Entropy: Measuring Inchoate Harm | 1749 |
| 4. The Need to Regulate Before Completed Harm | 1750 |
| B. Wait for Technology to Save Us | 1751 |
| 1. Why Not to Expect a Major Breakthrough | 1752 |
| a. Utility and Privacy: Two Concepts at War | 1752 |
| b. The Inverse and Imbalanced Relationship | 1753 |
| 2. The Prospect of Something Better Than Release-and-Forget | 1755 |
| 3. The Limitations of the Improved Techniques | 1756 |
| C. Ban Reidentification | 1758 |
| IV. RESTORING BALANCE TO PRIVACY LAW AFTER THE FAILURE OF ANONYMIZATION | 1759 |

| | |
|---|------|
| A. Which Database Owners Should We Regulate Anew? | 1759 |
| B. Regulatory Principles | 1761 |
| 1. From Math to Sociology | 1761 |
| 2. Support for Both Comprehensive and Contextual Regulation | 1762 |
| C. The Test | 1764 |
| 1. Five Factors for Assessing the Risk of Privacy Harm | 1765 |
| 2. Applying the Test | 1768 |
| D. Two Case Studies | 1769 |
| 1. Health Information | 1769 |
| 2. IP Addresses and Internet Usage Information | 1771 |
| a. Are IP Addresses Personal? | 1772 |
| b. Should the Data Protection Directive Cover Search Queries? | 1774 |
| CONCLUSION | 1776 |

INTRODUCTION

Imagine a database packed with sensitive information about many people. Perhaps this database helps a hospital track its patients, a school its students, or a bank its customers. Now imagine that the office that maintains this database needs to place it in long-term storage or disclose it to a third party without compromising the privacy of the people tracked. To eliminate the privacy risk, the office will anonymize the data, consistent with contemporary, ubiquitous data-handling practices.

First, it will delete personal identifiers like names and social security numbers. Second, it will modify other categories of information that act like identifiers in the particular context—the hospital will delete the names of next of kin, the school will excise student ID numbers, and the bank will obscure account numbers.

What will remain is a best-of-both-worlds compromise: Analysts will still find the data useful, but unscrupulous marketers and malevolent identity thieves will find it impossible to identify the people tracked. Anonymization will calm regulators and keep critics at bay. Society will be able to turn its collective attention to other problems because technology will have solved this one. Anonymization ensures privacy.

Unfortunately, this rosy conclusion vastly overstates the power of anonymization. Clever adversaries can often *reidentify* or *deanonymize* the people hidden in an anonymized database. This Article is the first to comprehensively incorporate an important new subspecialty of computer science, reidentification

science, into legal scholarship.¹ This research unearths a tension that shakes a foundational belief about data privacy: *Data can be either useful or perfectly anonymous but never both.*

Reidentification science disrupts the privacy policy landscape by undermining the faith we have placed in anonymization. This is no small faith, for technologists rely on it to justify sharing data indiscriminately and storing data perpetually, while promising users (and the world) that they are protecting privacy. Advances in reidentification expose these promises as too often illusory.

These advances should trigger a sea change in the law because nearly every information privacy law or regulation grants a get-out-of-jail-free card to those who anonymize their data. In the United States, federal privacy statutes carve out exceptions for those who anonymize.² In the European Union, the famously privacy-protective Data Protection Directive extends a similar safe harbor through the way it defines "personal data."³ Yet reidentification science exposes the underlying promise made by these laws—that anonymization protects privacy—as an empty one, as broken as the technologists' promises. At the very least, lawmakers must reexamine every privacy law, asking whether the power of reidentification and fragility of anonymization have thwarted their original designs.

The power of reidentification also transforms the public policy debate over information privacy. Today, this debate centers almost entirely on squabbles over magical phrases like "personally identifiable information" (PII) or "personal data." Advances in reidentification expose how thoroughly these phrases miss the point. Although it is true that a malicious adversary can use PII such as a name or social security number to link data to identity, as it turns out, the adversary can do the same thing using information that nobody would classify as personally identifiable.

1. A few legal scholars have considered the related field of statistical database privacy. E.g., Douglas J. Sylvester & Sharon Lohr, *The Security of Our Secrets: A History of Privacy and Confidentiality in Law and Statistical Practice*, 83 DENV. U. L. REV. 147 (2005); Douglas J. Sylvester & Sharon Lohr, *Counting on Confidentiality: Legal and Statistical Approaches to Federal Privacy Law After the USA PATRIOT Act*, 2005 WIS. L. REV. 1033. In addition, a few law students have discussed some of the reidentification studies discussed in this Article, but without connecting these studies to larger questions about information privacy. See, e.g., Benjamin Charkow, Note, *The Control Over the De-Identification of Data*, 21 CARDOZO ARTS & ENT. L.J. 195 (2003); Christine Porter, Note, *Re-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information*, 5 SMITHLER J.L. COM. & TECH. 3 (2008) (discussing the AOL and Netflix stories).

2. See *infra* Part II.B.

3. Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 [hereinafter EU Data Protection Directive].

How many other people in the United States share your specific combination of ZIP code, birth date (including year), and sex? According to a landmark study, for 87 percent of the American population, the answer is zero; these three pieces of information uniquely identify each of them.⁴ How many users of the Netflix movie rental service can be uniquely identified by when and how they rated any three of the movies they have rented? According to another important study, a person with this knowledge can identify more than 80 percent of Netflix users. Prior to these studies, nobody would have classified ZIP code, birth date, sex, or movie ratings as PII. As a result, even after these studies, companies have disclosed this kind of information connected to sensitive data in supposedly anonymized databases, with absolute impunity.

These studies and others like them sound the death knell for the idea that we protect privacy when we remove PII from our databases. This idea, which has been the central focus of information privacy law for almost forty years, must now yield to something else. But to what?

In search of privacy law's new organizing principle, we can derive from reidentification science two conclusions of great importance:

First, the power of reidentification will create and amplify privacy harms. Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal. Our enemies will find it easier to connect us to facts that they can use to blackmail, harass, defame, frame, or discriminate against us. Powerful reidentification will draw every one of us closer to what I call our personal "databases of ruin."⁶

Second, regulators can protect privacy in the face of easy reidentification only at great cost. Because the utility and privacy of data are intrinsically connected, no regulation can increase data privacy without also decreasing data

4. Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Laboratory for Intel Data Privacy, Working Paper LIDAP-WP4, 2000). For more on this study, see *infra* Part I.B.1.b. More recently, Philippe Golle revisited Dr. Sweeney's study, and recalculated the statistics based on year 2000 census data. Dr. Golle could not replicate the earlier 87 percent statistic, but he did calculate that 61 percent of the population in 1990 and 63 percent in 2000 were uniquely identified by ZIP, birth date, and sex. Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y 77, 78 (2006).

5. Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, in *PROC. OF THE 2008 IEEE SYM. ON SECURITY AND PRIVACY* 111, 121 [hereinafter *Netflix Prize Study*]. For more on this study, see *infra* Part I.B.1.c.

6. See *infra* Part III.A.

utility. No useful database can ever be perfectly anonymous, and as the utility of data increases, the privacy decreases.

Thus, easy, cheap, powerful reidentification will cause significant harm that is difficult to avoid. Faced with these daunting new challenges, regulators must find new ways to measure the risk to privacy in different contexts. They can no longer model privacy risks as a wholly scientific mathematical exercise, but instead must embrace new models that take messier human factors like motive and trust into account. Sometimes, they may need to resign themselves to a world with less privacy than they would like. But more often, regulators should prevent privacy harm by squeezing and reducing the flow of information in society, even though in doing so they may need to sacrifice, at least a little, important counter values like innovation, free speech, and security.

The Article proceeds in four Parts. Part I describes the dominant role anonymization plays in contemporary data privacy practices and debates. It surveys the recent, startling advances in reidentification science, telling stories of how sophisticated data handlers—America Online, the state of Massachusetts, and Netflix—suffered spectacular, surprising, and embarrassing failures of anonymization. It then looks closely at the science of reidentification, borrowing heavily from a computer science literature heretofore untapped by legal scholars. Part II reveals how these powerful advances in reidentification thwart the aims of nearly every privacy law and regulation. Part III considers three simple and appealing responses to these imbalances but ultimately rejects them as insufficient and incomplete. Finally, Part IV offers a way forward, proposing a test for deciding when to impose new privacy restrictions on information flow and demonstrating the test with examples from health and internet privacy.

I. ANONYMIZATION AND REIDENTIFICATION

A. The Past: Robust Anonymization

Something important has changed. For decades, technologists have believed that they could robustly protect people's privacy by making small changes to their data, using techniques surveyed below. I call this the *robust anonymization assumption*. Embracing this assumption, regulators and technologists have promised privacy to users, and in turn, privacy is what users have come to expect. Today, anonymization is ubiquitous.

But in the past fifteen years, computer scientists have established what I call the *easy reidentification result*, which proves that the robust anonymization

assumption is deeply flawed—not fundamentally incorrect, but deeply flawed. By undermining the robust anonymization assumption, easy reidentification will topple the edifices of promise and expectation we have built upon anonymization. The easy reidentification result will also wreak havoc on our legal systems because our faith in robust anonymization has thoroughly infiltrated our privacy laws and regulations as Part II explores. But before we deploy the wrecking balls, this Part reviews the story of how we built these grand structures, to explain what we are about to lose.

1. Ubiquitous Anonymization

Anonymization plays a central role in modern data handling, forming the core of standard procedures for storing or disclosing personal information. What is anonymization, why do people do it, and how widespread is it?

a. The Anonymization/Reidentification Model

Let us begin with terminology. A person or entity, the data administrator, possesses information about individuals, known as data subjects. The data administrator most often stores the information in an electronic database, but it may also maintain information in other formats, such as traditional paper records.

Data administrators try to protect the privacy of data subjects by anonymizing data. Although I will later argue against using this term,⁷ I am not quite ready to let it go, so for now, anonymization is a process by which information in a database is manipulated to make it difficult to identify data subjects.

Database experts have developed scores of different anonymization techniques, which vary in their cost, complexity, ease of use, and robustness. For starters, consider a very common technique: suppression.⁸ A data administrator suppresses data by deleting or omitting it entirely. For example, a hospital data administrator tracking prescriptions will suppress the names of patients before sharing data in order to anonymize it.

The reverse of anonymization is reidentification or deanonymization.⁹ A person, known in the scientific literature as an adversary,¹⁰ reidentifies

7. See *infra* Part II.C.2

8. See Latanya Sweeney, *Achieving k-Anonymity Privacy Protection Using Generalization and Suppression*, 10 INT'L J. ON UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 571, 572 (2002).

9. E.g., *Netflix Prize Study*, *supra* note 5, at 111–12

10. *Id.*

anonymized data by linking anonymized records to outside information, hoping to discover the true identity of the data subjects.

b. The Reasons to Anonymize

Data administrators anonymize to protect the privacy of data subjects when storing or disclosing data. They disclose data to three groups. First, they release data to third parties: For example, health researchers share patient data with other health researchers,¹¹ websites sell transaction data to advertisers,¹² and phone companies can be compelled to disclose call logs to law enforcement officials.¹³ Second, administrators sometimes release anonymized data to the public.¹⁴ Increasingly, administrators do this to engage in what is called crowdsourcing—attempting to harness large groups of volunteer users who can analyze data more efficiently and thoroughly than smaller groups of paid employees.¹⁵ Third, administrators disclose anonymized data to others within their organization.¹⁶ Particularly within large organizations, data collectors may want to protect data subjects' privacy even from others in the organization.¹⁷ For example, large banks may want to share some data with their marketing departments, but only after anonymizing it to protect customer privacy.

Lawrence Lessig's four regulators of behavior—norms and ethics, the market, architecture, and law—each compel administrators to anonymize.¹⁸ Anonymization norms and ethics often operate through best practice documents that recommend anonymization as a technique for protecting privacy. For example, biomedical guidelines often recommend coding genetic

11. National Institute of Health, HIPAA Privacy Rules for Researchers, <http://privacyruleandresearch.nih.gov/faq.asp> (last visited June 12, 2010).

12. E.g., Posting of Susan Wojcicki, Vice President, Product Management to The Official Google Blog, Making Ads More Interesting, <http://googleblog.blogspot.com/2009/0/making-ads-more-interesting.html> (Mar. 11, 2009, 2:01 EST) (announcing a new Google initiative to tailor ads to "the types of sites you visit and the pages you view").

13. E.g., *In re Application of United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (granting the government the authority to compel a provider to provide information suggesting the location of a customer's cell phone).

14. See *infra* Part I B 1 (describing three public releases of databases).

15. See CLAY SHIRKY, *HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS* (2008); JAMES SUROWIECKI, *THE WISDOM OF CROWDS* (2004).

16. See Posting of Philip Lensen to Google Blogscoped, Google-Internal Data Restrictions, <http://blogscoped.com/archive/2007-06-27-n27.html> (June 27, 2007) (detailing how Google and Microsoft limit internal access to sensitive data).

17. See *id.*

18. See LAWRENCE LESSIG, *CODE VERSION 2.0*, at 123 (2006) (listing four regulators of online behavior: markets, norms, laws, and architecture).

data—associating stored genes with nonidentifying numbers—to protect privacy.¹⁹ Other guidelines recommend anonymization in contexts such as electronic commerce,²⁰ internet service provision,²¹ data mining,²² and national security data sharing.²³ Academic researchers rely heavily on anonymization to protect human research subjects, and their research guidelines recommend anonymization generally,²⁴ and specifically in education,²⁵ computer network monitoring,²⁶ and health studies.²⁷ Professional statisticians are duty-bound to anonymize data as a matter of professional ethics.²⁸

Market pressures sometimes compel businesses to anonymize data. For example, companies like mint.com and wesabe.com provide web-based personal finance tracking and planning.²⁹ One way these companies add value is by aggregating and republishing data to help their customers compare their spending with that of similarly situated people.³⁰ To make customers comfortable with this type of data sharing, both mint.com and wesabe.com promise to anonymize data before sharing it.³¹

Architecture, defined in Lessig's sense as technological constraints,³² often forces anonymization, or at least makes anonymization the default choice. As one example, whenever you visit a website, the distant computer with which you communicate—also known as the web server—records some information

19. Roberto Andorno, *Population Genetic Databases: A New Challenge to Human Rights*, in *ETHICS AND LAW OF INTELLECTUAL PROPERTY* 39 (Christian Lenk, Nils Hoppe & Roberto Andorno eds., 2007).

20. ALEX DERSON & LARRY DUBOV, *MASTER DATA MANAGEMENT AND CUSTOMER DATA INTEGRATION FOR A GLOBAL ENTERPRISE* 338–39 (2007).

21. See *infra* Part II.A.3.b.

22. G.K. GUPTA, *INTRODUCTION TO DATA MINING WITH CASE STUDIES* 432 (2006).

23. MARKLE FOUND. TASK FORCE, *CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY* 144 (2003), available at http://www.markle.org/downloadable_assets/task_force_report2_full_report.pdf.

24. See THE SAGE ENCYCLOPEDIA OF QUALITATIVE RESEARCH METHODS 196 (Lisa M. Given ed., 2008) (entry for "Data Security").

25. LOUIS COHEN ET AL., *RESEARCH METHODS IN EDUCATION* 189 (2003).

26. See R.oming Pang et al., *The Devil and Pocket Trace Anonymization*, 36 *COMP. COMM. REV.* 29 (2006).

27. INST. OF MED., *PROTECTING DATA PRIVACY IN HEALTH SERVICES RESEARCH* 178 (2000).

28. European Union Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01246/07/EN WP 136, at 21 (June 20, 2007) [hereinafter 2007 Working Party Opinion], available at http://ec.europa.eu/justice_home/isj/privacy/docs/wpdocs/2007/wp136_en.pdf.

29. See Eric Benderoff, *Spend and Save the Social Way—Personal Technology*, SEATTLE TIMES, Nov. 8, 2008, at A9.

30. See Carolyn Y. Johnson, *Online Social Networking Meets Personal Finance*, N.Y. TIMES, Aug. 7, 2007, available at <http://www.nytimes.com/2007/08/07/technology/07iht-debt.1.7013213.html>.

31. See, e.g., Wesabe, *Security and Privacy*, <http://www.wesabe.com/page/security> (last visited June 12, 2010); Mint.com, *How Mint Personal Finance Management Protects Your Financial Safety*, <http://www.mint.com/privacy> (last visited June 12, 2010).

32. LESSIG, *supra* note 18, at 4.

about your visit into what is called a log file." The vast majority of web servers collect much less than the maximum amount of information available about your visit, not due to the principled privacy convictions of their owners, but because the software saves only a limited amount of information by default.³³

c. Faith in Anonymization

Many defend the privacy-protecting power of anonymization and hold it out as a best practice despite evidence to the contrary. In one best practices guide, the authors, after cursorily acknowledging concerns about the power of anonymization conclude that, "[w]hile we recognize that [reidentification] is a remote possibility in some situations, in most cases genetic research data anonymization will help to ensure confidentiality."³⁵ Similarly, Google has said, "[i]t is difficult to guarantee complete anonymization, but we believe [Google's log file anonymization techniques] will make it very unlikely users could be identified."³⁶

Government officials and policymakers embrace anonymization as well. Two influential data mining task forces have endorsed anonymization. In 2004, the Technology and Privacy Advisory Committee (TAPAC), a Defense Department-led group established in the wake of controversy over the government's Total Information Awareness program, produced an influential report about government data mining.³⁷ The report recommends anonymization "whenever practicable" and thus restricts all of its other recommendations only to databases that are not "known or reasonably likely to include personally identifiable information."³⁸

Likewise, the Markle Foundation task force, which included among its members now-Attorney General Eric Holder, produced a similar report.³⁹ Like TAPAC, the Markle Foundation group concluded that "anonymizing technologies could be employed to allow analysts to perform link analysis among data sets without disclosing personally identifiable information . . . [so]

33. STEPHEN SPAINKOUR & ROBERT ECKSTEIN, WEBMASTER IN A NUTSHELL 458-59 (2002).

34. Apache, Apache HTTP Server Version 1.3 Log Files, <http://httpd.apache.org/docs/1.3/logs.html> (last visited June 12, 2010) (describing the default "common log format" which logs less information than the alternative "combined log format").

35. ADIL E. SHAMMOO & DAVID B. RESNICK, RESPONSIBLE CONDUCT OF RESEARCH 302 (2009).

36. Chris Seighean, *Debunking Google's Log Anonymization Propaganda*, SURVEILLANCE STATE, CNET NEWS, Sept. 11, 2008, http://news.cnet.com/8301-13739_3-10038963-40.html.

37. TECHNOLOGY & PRIVACY ADVISORY COMM., REPORT: SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 35-36 (2004), available at <http://www.cdt.org/security/usapatriot/20040700tapac.pdf>.

38. *Id.* at 50 (Recommendation 2.2).

39. See MARKLE FOUND. TASK FORCE, *supra* note 23, at 34.

analysts can perform their jobs and search for suspicious patterns without the need to gain access to personal data until they make the requisite showing for disclosure."⁴⁰

Many legal scholars share this faith in anonymization.⁴¹ Ira Rubinstein, Ronald Lee, and Paul Schwartz state a "consensus view" that "[w]ith the goal of minimizing the amount of personal information revealed in the course of running pattern-based searches, the anonymization of data (such as names, addresses, and social security numbers) is essential."⁴² Barbara Evans, a prominent medical privacy scholar, speaks about "anonymized" data "that have had patient identifiers completely and irrevocably removed before disclosure, such that future reidentification would be impossible."⁴³ Many other legal scholars have made similar claims premised on deep faith in robust anonymization.⁴⁴ The point is not to criticize or blame these people for trusting anonymization; as we will see, even computer scientists have been surprised by the success of recent attacks on anonymization.

2. Anonymization Techniques: The Release-and-Forget Model

How do people anonymize data? From among the scores of different anonymization techniques, I will focus on an important and large subset that I call release-and-forget anonymization.⁴⁵ As the name suggests, when a data administrator practices these techniques, she releases records—either publicly,

40. *Id.* at 34.

41. Regulators do too. See *infra* Part III.A (listing laws and regulations that assume robust anonymization).

42. Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 266, 263 (2006).

43. Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. 585, 619–20 (2009). Professor Evans has clarified that the quote did not reflect her personal opinions about the feasibility of definitive anonymization but rather reflected how the term 'anonymization' has commonly been understood by regulators and others in bioethics. Email from Barbara Evans, Assoc. Professor, Univ. of Houston Law Ctr., to Paul Ohm, Assoc. Professor, Univ. of Colorado Law Sch. (July 21, 2010) (on file with author).

44. See, e.g., Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV C.R.-C.L. L. REV. 435, 487 (2008); Matthew P. Gordon, *A Legal Duty to Disclose Individual Research Findings to Research Subjects?*, 64 FOOD & DRUG L.J. 225, 253–59 (2009); Bartha Maria Knoppers et al., *Ethical Issues in Secondary Uses of Human Biological Material From Mass Disasters*, 34 J.L. MED. & ETHICS 352, 353 (2006); Susan M. Wolf et al., *Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations*, 36 J.L. MED. & ETHICS 219, 226–27 (2008); Irfan Tuckli, Comment, *Transatlantic Turbulence: The Passenger Name Record Conflict*, 45 HOUS. L. REV. 587, 618–19 (2008).

45. Other means of making data more anonymous include releasing only aggregated statistics, interactive techniques, in which administrators answer directed questions on behalf of researchers, instead of releasing data in its entirety; and "differential privacy" techniques, which protect privacy by adding carefully calibrated noise to the data. See discussion *infra* Part III.B.2.

privately to a third party, or internally within her own organization—and then she forgets, meaning she makes no attempt to track what happens to the records after release. Rather than blithely put her data subjects at risk, before she releases, she modifies some of the information.

I focus on release-and-forget anonymization for two reasons. First, these techniques are widespread.⁴⁶ Because they promise privacy while allowing the broad dissemination of data, they give data administrators everything they want without any compromise, and data administrators have embraced them.⁴⁷ Second, these techniques are often flawed. Many of the recent advances in the science of reidentification target release-and-forget anonymization in particular.⁴⁸

Consider some common release-and-forget techniques.⁴⁹ First, we need a sample database to anonymize, a simplified and hypothetical model of a hospital's database for tracking visits and complaints.⁵⁰

TABLE 1. Original (Nonanonymized) Data

| Name | Race | Birth Date | Sex | ZIP Code | Complaint |
|--------|-------|------------|--------|----------|-----------------|
| Sean | Black | 9/20/1965 | Male | 02141 | Short of breath |
| Daniel | Black | 2/14/1965 | Male | 02141 | Chest pain |
| Kate | Black | 10/23/1965 | Female | 02138 | Painful eye |
| Marion | Black | 8/24/1965 | Female | 02138 | Whooping |
| Helen | Black | 11/7/1964 | Female | 02138 | Aching joints |
| Reese | Black | 12/1/1964 | Female | 02138 | Chest pain |
| Foresa | White | 10/23/1964 | Male | 02138 | Short of breath |
| Hilary | White | 3/15/1965 | Female | 02139 | Hypertension |
| Philip | White | 8/13/1964 | Male | 02139 | Aching joints |
| Jamie | White | 5/5/1964 | Male | 02139 | Fever |
| Sean | White | 2/13/1967 | Male | 02138 | Vomiting |
| Adrien | White | 3/21/1967 | Male | 02138 | Back pain |

46. See Lata S. Lakshmanan & Raymond T. Ng, *On Disclosure Risk: Analysis of Anonymized Datasets in the Presence of Prior Knowledge*, 2 ACM TRANSACTIONS ON KNOWLEDGE DISCOVERY FROM DATA 13, 13:2 (2008) ("Among the well-known transformation techniques, anonymization is arguably the most common").

47. *Id.* ("Compared with other transformation techniques, anonymization is simple to carry out, as mapping objects back and forth is easy").

48. See Justin Buckell & Vitaly Shmatikov, *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, in 2008 KNOWLEDGE DISCOVERY & DATA MINING CONF. 70, 70.

49. The following discussion is only a survey; it will make an expert of no one.

50. All of the hypothetical data in this table aside from the "Name" column comes from a paper by Latanya Sweeney. Sweeney, *supra* note 8, at 567 fig. 4. Where the first name comes from is left as an exercise for the reader.

Using standard terminology, we call this collection of data a table; each row is a row or record, each column is a column, field, or attribute, identified by a label (in bold) called a field name or attribute name; each record has a particular value for a given attribute.⁵¹

To protect the privacy of the people in this table, the hospital database administrator will take the following steps before releasing this data:

Singling Out Identifying Information: First, the administrator will single out any fields she thinks one can use to identify individuals. Often, she will single out not only well-known identifiers like name and social security number, but combinations of fields that when considered together might link a record in the table to a patient's identity.⁵² Sometimes an administrator will select the potentially identifying fields herself, either intuitively (by isolating types of data that seem identifying) or analytically (by looking for uniqueness in the particular data). For example, no two people in our data set share a birth date, so the administrator must treat birth date as an identifier.⁵³ If she did not, then anyone who knew Forest's birth date (and who knew Forest had been admitted to the hospital) would be able to find Forest in the anonymized data.⁵⁴

In other cases, an administrator will look to another source—such as a statistical study, company policy, or government regulation—to decide whether or not to treat a particular field as identifying. In this case, assume the administrator decides, based on one of these sources, to treat the following four fields as potential identifiers: name, birth date, sex, and ZIP code.⁵⁵

Suppression: Next, the administrator will modify the identifying fields. She might suppress them, removing the fields from the table altogether.⁵⁶ In our example, the administrator might delete all four potential identifiers, producing this table:

51. GAVIN POWELL, *BEGINNING DATABASE DESIGN*, 33–41 (2005).

52. Claudio Bettini et al., *The Role of Quasi-Identifiers in k-Anonymity Revisited* (DICo Univ. Milan Tech. Rep. RT-11-06, July 2006).

53. See *id.* Because these sorts of identifiers do not link directly to identity, researchers sometimes refer to them as quasi-identifiers.

54. That large numbers of people could know Forest's birth date is far from an idle worry. Today, more than ever, people are sharing this kind of information widely. For example, "at least 10 million U.S. residents make publicly available or inferable their birthdate information on their [social networking] online profiles." Alessandro Acquisti & Ralph Gross, *SSN Study-FAQ*, <http://www.heinz.cmu.edu/~acquisti/ssnstudy> (last visited June 12, 2010).

55. See *infra* Part I B.1.b (discussing research about using the combination of ZIP code, birth date, and sex as an identifier).

56. Sweeney, *supra* note 8, at 3.

TABLE 2: Suppressing Four Identifier Fields

| Race | Complaint |
|-------|-----------------|
| Black | Short of breath |
| Black | Chest pain |
| Black | Painful eye |
| Black | Wheezing |
| Black | Aching joints |
| Black | Chest pain |
| White | Short of breath |
| White | Hypertension |
| White | Aching joints |
| White | Fever |
| White | Vomiting |
| White | Back pain |

Here we first encounter a fundamental tension. On the one hand, with this version of the data, we should worry little about privacy, even if one knows Forest's birth date, sex, ZIP code, and race, one still cannot learn Forest's complaint. On the other hand, aggressive suppression has rendered this data almost useless for research.⁵⁷ Although a researcher can use the remaining data to track the incidence of diseases by race, because age, sex, and residence have been removed, the researcher will not be able to draw many other interesting and useful conclusions.

Generalization: To better strike the balance between utility and privacy, the anonymizer might generalize rather than suppress identifiers.⁵⁸ This means she will alter rather than delete identifier values to increase privacy while preserving utility. For example, the anonymizer may choose to suppress the name field, generalize the birth date to only the year of birth, and generalize ZIP codes by retaining only the first three digits.⁵⁹ The resulting data would look like this:

57. See *infra* Part III.B.1 (discussing the relationship between utility and privacy).

58. Sweetney, *supra* note 8, at 3.

59. Under the HIPAA Privacy Rule, these three changes would qualify the resulting table as deidentified health information. See U.S. Health & Human Services, Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160, 164 (2009). For more on HIPAA and the Privacy Rule, see *infra* Part II.A.3 a.

TABLE 3: Generalized

| Race | Birth Year | Sex | ZIP Code* | Complaint |
|-------|------------|--------|-----------|-----------------|
| Black | 1965 | Male | 021* | Short of breath |
| Black | 1965 | Male | 021* | Chest pain |
| Black | 1965 | Female | 021* | Painful eye |
| Black | 1965 | Female | 021* | Wheezing |
| Black | 1964 | Female | 021* | Aching joints |
| Black | 1964 | Female | 021* | Chest pain |
| White | 1964 | Male | 021* | Short of breath |
| White | 1965 | Female | 021* | Hypertension |
| White | 1964 | Male | 021* | Aching joints |
| White | 1964 | Male | 021* | Fever |
| White | 1967 | Male | 021* | Vomiting |
| White | 1967 | Male | 021* | Back pain |

Now, even someone who knows Forest's birth date, ZIP code, sex, and race will have trouble plucking out Forest's specific complaint. The records in this generalized data (Table 3) are more difficult to reidentify than they were in the original data (Table 1), but researchers will find this data much more useful than the suppressed data (Table 2).

Aggregation: Finally, to better understand what qualifies as release-and-forget anonymization, consider a commonly used technique that does not obey release-and-forget. Quite often, an analyst needs only summary statistics, not raw data. For decades, statisticians have investigated how to release aggregate statistics while protecting data subjects from reidentification.⁶⁰ Thus, if researchers only need to know how many men complained of shortness of breath, data administrators could release this

TABLE 4: Aggregate Statistic

| | |
|---------------------|---|
| Men Short of Breath | 2 |
|---------------------|---|

60. E.g., Nabil R. Adam & John C. Wortmann, *Security-Control Methods for Statistical Databases: A Comparative Study*, 21 ACM COMPUTING SURVEYS 515 (1989); Tore Dalenius, *Towards a Methodology for Statistical Disclosure Control*, 15 STATISTISK TIDSKRIFT 429 (1977) (Swed.); I.P. Fellegi, *On the Question of Statistical Confidentiality*, 67 J. AM. STAT. ASS'N 7 (1972).

As it happens, Forest is one of the two men described by this statistic—he complained about shortness of breath—but without a lot of additional information, one would never know. His privacy is secure.⁶¹

Privacy lawyers tend to refer to release-and-forget anonymization techniques using two other names: deidentification⁶² and the removal of personally identifiable information (PII).⁶³ Deidentification has taken on special importance in the health privacy context. Regulations implementing the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) expressly use the term, exempting health providers and researchers who deidentify data before releasing it from all of HIPAA's many onerous privacy requirements.⁶⁴

B. The Present and Future: Easy Reidentification

Until a decade ago, the robust anonymization assumption worked well for everybody involved. Data administrators could protect privacy when sharing data with third parties; data subjects could rest assured that their secrets would remain private; legislators could balance privacy and other interests (such as the advancement of knowledge) by deregulating the trade in anonymized records;⁶⁵ and regulators could easily divide data handlers into two groups: the responsible (those who anonymized) and the irresponsible (those who did not).

About fifteen years ago, researchers started to chip away at the robust anonymization assumption, the foundation upon which this state of affairs has been built. Recently, however, they have done more than chip away; they have essentially blown it up, casting serious doubt on the power of anonymization, proving its theoretical limits and establishing what I call the easy reidentification result. This is not to say that all anonymization techniques fail to protect privacy—some techniques are very difficult to reverse—but researchers have learned more than enough already for us to reject anonymization as a privacy-providing panacea.

61. For additional discussion of privacy techniques other than release-and-forget, see *infra* Part III.B.2.

62. National Institutes of Health, *De-identifying Protected Health Information Under the Privacy Rule*, http://privacyruleandresearch.nih.gov/pr_08.asp (last visited June 12, 2010).

63. ERIKA MCCALLISTER ET AL., NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. NO. 800-122, *GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)* (2010), available at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

64. 45 C.F.R. §§ 164.502(d)(2), 164.514(a)–(b) (2009). See *infra* Part II.A.1.a.

65. See *infra* II.A.

1. How Three Anonymized Databases Were Undone

Consider three recent, spectacular failures of anonymization. In each case, a sophisticated entity placed unjustified faith in weak, release-and-forget anonymization. These stories, which I will use as examples throughout this Article, provide two important lessons: They demonstrate the pervasiveness of release-and-forget anonymization even among supposedly sophisticated data administrators, and they demonstrate the peril of this kind of anonymization in light of recent advances in reidentification.

a. The AOL Data Release

On August 3, 2006, America Online (AOL) announced a new initiative called "AOL Research."⁶⁶ To "embrace[] the vision of an open research community," AOL Research publicly posted to a website twenty million search queries for 650,000 users of AOL's search engine, summarizing three months of activity.⁶⁷ Researchers of internet behavior rejoiced to receive this treasure trove of information, the kind of information that is usually treated by search engines as a closely guarded secret.⁶⁸ The euphoria was short-lived, however, as AOL and the rest of the world soon learned that search engine queries are windows to the soul.

Before releasing the data to the public, AOL had tried to anonymize it to protect privacy. It suppressed any obviously identifying information such as AOL user name and IP address in the released data.⁶⁹ In order to preserve the usefulness of the data for research, however, it replaced these identifiers with unique identification numbers that allowed researchers to correlate different searches to individual users.⁷⁰

In the days following the release, bloggers pored through the data spotlighting repeatedly the nature and extent of the privacy breach. These bloggers chased two different prizes, either attempting to identify users or

66. Posting of Abdur Chowdhury, cabdur@aol.com, to SIGIR-IRList, irlist-editor@acm.org, http://sitaka.cs.muc.edu/xshen/aol/20060803_SIG-IRListEmail.txt (last visited July 19, 2010).

67. *Id.* Others have reported that the data contained thirty-six million entries. Paul Boutin, *You Are What You Search*, SLATE, Aug. 11, 2006, <http://www.slate.com/id/2147590>.

68. See Katie Hattner, *Researchers Yearn to Use AOL Log, but They Hesitate*, N.Y. TIMES, Aug. 23, 2006, at C1 (describing the difficulty that academic researchers experience accessing raw search data).

69. See Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1. IP addresses, discussed *infra* in Part II A.3 b, are numbers that identify computers on the internet and can be used to track internet activity.

70. Barbaro & Zeller, Jr., *supra* note 69.

"hunt[ing] for particularly entertaining or shocking search histories."⁷¹ Thanks to this blogging and subsequent news reporting, certain user identification numbers have become sad little badges of infamy, associated with pitiful or chilling stories. User "No. 3505202 ask[ed] about 'depression and medical leave.' No. 7263042 type[d] 'fear that spouse contemplating cheating.'"⁷² User 17556639 searched for "how to kill your wife" followed by a string of searches for things like "pictures of dead people" and "car crash photo."⁷³

While most of the blogosphere quickly and roundly condemned AOL,⁷⁴ a few bloggers argued that the released data, while titillating, did not violate privacy because nobody had linked actual individuals with their anonymized queries.⁷⁵ This argument was quickly silenced by *New York Times* reporters Michael Barbaro and Tom Zeller, who recognized clues to User 4417749's identity in queries such as "'landscapers in Lilburn, Ga,' several people with the last name Arnold and 'homes sold in shadow lake subdivision gwinnett county georgia'"⁷⁶ They quickly tracked down Thelma Arnold, a sixty-two-year-old widow from Lilburn, Georgia who acknowledged that she had authored the searches, including some mildly embarrassing queries such as "numb fingers," "60 single men" and "dog that urinates on everything."⁷⁷

The fallout was swift and crushing. AOL fired the researcher who released the data and also his supervisor.⁷⁸ Chief Technology Officer Maureen Govern resigned.⁷⁹ The fledgling AOL Research division has been silenced, and a year after the incident, the group still had no working website.⁸⁰

71. *Id.* These twin goals demonstrate an important information dichotomy revisited later: When someone talks about the sensitivity of data, they may mean that the information can cause harm if disclosed, or they may mean that the information can be used to link anonymized information to identity. As we will see, regulators often misunderstand the difference between these two classes of information. See *infra* Part II.A.

72. See Barbaro & Zeller, Jr., *supra* note 69.

73. Markus Fird, *AOL Search Data Shows Users Planning to Commit Murder, Paradigm Shift Blog* (Aug. 7, 2006), <http://pk.nryoffish.wordpress.com/2006/08/07/aol-search-data-shows-users-planning-to-commit-murder>.

74. See, e.g., Posting of Michael Arrington to TechCrunch, *AOL Proudly Releases Massive Amounts of Private Data* (Aug. 6, 2006), <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/> ("The utter stupidity of this is staggering.").

75. Greg Linden, for example, complained that "no one actually has come up with an example where someone could be identified. Just the theoretical possibility is enough to create a privacy firestorm in some people's minds." Greg Linden, *A Chance to Play With Big Data: Geeking With Creq*, <http://glinden.blogspot.com/2006/08/a-chance-to-play-with-big-data.html> (Aug. 4, 2006, 19:53 PST).

76. Barbaro & Zeller, Jr., *supra* note 69.

77. *Id.*

78. Tom Zeller, Jr., *AOL Executive Quits After Posting of Search Data*, *N.Y. TIMES*, Aug. 22, 2006, <http://www.nytimes.com/2006/08/22/technology/22iht-aol.2558731.html>.

79. *Id.*

80. Chris Schoonin, *AOL, Netflix and the End of Open Access to Research Data*, *Surveillance State*, CNET NEWS, Nov. 30, 2007, http://news.cnet.com/8301-13739_3-9826608-46.html.

b.ZIP, Sex, and Birth Date

Recall from the Introduction the study by Latanya Sweeney, professor of computer science, who crunched 1990 census data and discovered that 87.1 percent of people in the United States were uniquely identified by their combined five-digit ZIP code, birth date (including year), and sex.⁸¹ According to her study, even less specific information can often reveal identity, as 53 percent of American citizens are uniquely identified by their city, birth date, and sex, and 18 percent by their county, birth date, and sex.⁸²

Like the reporters who discovered Thelma Arnold, Dr. Sweeney offered a hyper-salient example to drive home the power (and the threat) of reidentification techniques. In Massachusetts, a government agency called the Group Insurance Commission (GIC) purchased health insurance for state employees.⁸³ At some point in the mid-1990s, GIC decided to release records summarizing every state employee's hospital visits at no cost to any researcher who requested them.⁸⁴ By removing fields containing name, address, social security number, and other "explicit identifiers," GIC assumed it had protected patient privacy, despite the fact that "nearly one hundred attributes per" patient and hospital visit were still included, including the critical trio of ZIP code, birth date, and sex.⁸⁵

At the time that GIC released the data, William Weld, then-Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers.⁸⁶ In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data.⁸⁷ She knew that Governor Weld resided in Cambridge, Massachusetts, a city of fifty-four thousand residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge—a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor

81. Sweeney, *supra* note 4. A subsequent study placed the number at 61 percent (for 1990 census data) and 63 percent (for 2000 census data). Colle, *supra* note 4, at 1.

82. Sweeney, *supra* note 4.

83. Massachusetts Executive Office for Administration and Finance, *Who is the GIC?*, <http://mass.gov/gic> (follow "Who is the GIC?" hyperlink) (last visited June 15, 2010).

84. *Recommendations to Identify and Combat Privacy Problems in the Commonwealth: Hearing on H.R. 351 Before the H. Select Comm. on Information Security, 189th Sess. (Pa. 2005)* (statement of Latanya Sweeney, Associate Professor, Carnegie Mellon University), available at <http://dataprivacylab.org/dataprivacy/talks/Flick-05-10.html>.

85. *Id.*

86. Henry T. Greely, *The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks*, 8 ANN. REV. GENOMICS & HUM. GENETICS 343, 352 (2007).

87. *Id.*

Weld with ease. Only six people in Cambridge shared his birth date; only three were men, and of the three, only he lived in his ZIP code.⁸⁸ In a theatrical flourish, Dr. Sweeney sent the governor's health records (including diagnoses and prescriptions) to his office.⁸⁹

c. The Netflix Prize Data Study

On October 2, 2006, about two months after the AOL debacle, Netflix, the "world's largest online movie rental service," publicly released one hundred million records revealing how nearly a half-million of its users had rated movies from December 1999 to December 2005.⁹⁰ In each record, Netflix disclosed the movie rated, the rating assigned (from one to five stars), and the date of the rating.⁹¹ Like AOL and GIC, Netflix first anonymized the records, removing identifying information like usernames, but assigning a unique user identifier to preserve rating-to-rating continuity.⁹² Thus, researchers could tell that user 1337 had rated *Gattaca* a 4 on March 3, 2003, and *Minority Report* a 5 on November 10, 2003.

Unlike AOL, Netflix had a specific profit motive for releasing these records.⁹³ Netflix thrives by being able to make accurate movie recommendations; if Netflix knows, for example, that people who liked *Gattaca* will also like *The Lives of Others*, it can make recommendations that keep its customers coming back to the website.

To improve its recommendations, Netflix released the hundred million records to launch what it called the "Netflix Prize," a prize that took almost three years to claim.⁹⁴ The first team that used the data to significantly improve on Netflix's recommendation algorithm would win one million dollars.⁹⁵ As with the AOL release, researchers have hailed the Netflix Prize data release as a great boon for research, and many have used the competition to refine or develop important statistical theories.⁹⁶

88. Sweeney, *supra* note 4.

89. Greely, *supra* note 86.

90. The Netflix Prize Rules, <http://www.netflixprize.com/rules> (last visited June 12, 2010).

91. *Id.*

92. Netflix Prize FAQ, <http://www.netflixprize.com/faq> (last visited June 12, 2010) (answering the question, "Is there any customer information in the dataset that should be kept private?").

93. See Clive Thompson, *If You Liked This, You're Sure to Love That*, N.Y. TIMES MAG., Nov. 23, 2008, at 74, available at <http://www.nytimes.com/2008/11/23/magazine/23Netflix-t.html>.

94. Posting of Steve Lohr, *Netflix Challenge Ends, but Winner is in Doubt*, N.Y. TIMES BITS BLOG, <http://bits.blogs.nytimes.com/2009/07/27/netflix-challenge-ends-but-winner-is-in-doubt> (July 27, 2009, 16:59 EST).

95. See The Netflix Prize Rules, *supra* note 90.

96. See Thompson, *supra* note 93.

Two weeks after the data release, researchers from the University of Texas, Arvind Narayanan and Professor Vitaly Shmatikov, announced that "an attacker who knows only a little bit about an individual subscriber can easily identify this subscriber's record if it is present in the [Netflix Prize] dataset, or, at the very least, identify a small set of records which include the subscriber's record."⁹⁷ In other words, it is surprisingly easy to reidentify people in the database and thus discover all of the movies they have rated with only a little outside knowledge about their movie-watching preferences.

The resulting research paper is brimming with startling examples of the ease with which someone could reidentify people in the database, and has been celebrated and cited as surprising and novel to computer scientists.⁹⁸ If an adversary—the term used by computer scientists⁹⁹—knows the precise ratings a person in the database has assigned to six obscure movies,¹⁰⁰ and nothing else, he will be able to identify that person 84 percent of the time.¹⁰¹ If he knows approximately when (give or take two weeks) a person in the database has rated six movies, whether or not they are obscure, he can identify the person 99 percent of the time.¹⁰² In fact, knowing when ratings were assigned turns out to be so powerful that knowing only two movies a rating user has viewed (with the precise ratings and the rating dates give or take three days), an adversary can reidentify 68 percent of the users.¹⁰³

To summarize, the next time your dinner party host asks you to list your six favorite obscure movies, unless you want everybody at the table to know every movie you have ever rated on Netflix, say nothing at all.

To turn these abstract results into concrete examples, Narayanan and Shmatikov compared the Netflix rating data to similar data from the Internet

97. Arvind Narayanan & Vitaly Shmatikov, *How to Break the Anonymity of the Netflix Prize Dataset*, ARVIX, Oct. 16, 2006, at 1, <http://arxiv.org/abs/cs/0610105v1> (v.1) [hereinafter *Netflix Prize v1*]. Narayanan and Shmatikov eventually published the results in 2008. *Netflix Prize Study*, *supra* note 5.

98. In 2006, the paper was awarded the "Award for Outstanding Research in Privacy Enhancing Technologies" or PET Award, given jointly by Microsoft and the Privacy Commissioner of Ontario, Canada. Press Release, EMEA Press Ctr., Microsoft, *Privacy to the Test—Exploring the Limits of Online Anonymity and Accountability* (Jul. 23, 2008), http://www.microsoft.com/emea/presscentre/pressreleases/23072008_PETSEFS.mspx. E.g., Cynthia Dwork, *An Ad Omnia Approach to Defining and Achieving Private Data Analysis*, in *PRIVACY, SECURITY, AND TRUST IN KDID 1, 2* (2008), available at <http://www.springerlink.com/content/85g8155138612w06/fulltext.pdf>.

99. See *infra* Part I B.2.1.

100. By obscure movie, I mean a movie outside the top five hundred movies rated in the database, ranked by number of ratings given. See generally *Netflix Prize Study*, *supra* note 5.

101. *Id.* at 121, 122 fig.8. The authors emphasize that this result would apply to most of the rating users, as 90 percent of them rated five or more obscure movies and 60 percent rated ten or more obscure movies. *Id.* at 121 tbl.

102. *Id.* at 121, 120 fig.4.

103. *Id.*

Movie Database (IMDb),¹⁰⁴ a movie-related website that also gives users the chance to rate movies. Unlike Netflix, IMDb posts these ratings publicly on its website, as Amazon does with user-submitted book ratings.

Narayanan and Shmatikov obtained ratings for fifty IMDb users.¹⁰⁵ From this tiny sample,¹⁰⁶ they found two users who were identifiable, to a statistical near-certainty, in the Netflix database.¹⁰⁷ Because neither database comprised a perfect subset of the other, one could learn things from Netflix unknowable only from IMDb, and vice versa,¹⁰⁸ including some things these users probably did not want revealed. For example, the authors listed movies viewed by one user that suggested facts about his or her politics ("Fahrenheit 9/11"), religious views ("Jesus of Nazareth"), and attitudes toward gay people ("Queer as Folk").¹⁰⁹

Soon after it awarded the first Netflix Prize, the company announced that it would launch a second contest, one involving "demographic and behavioral data . . . includ[ing] information about renters' ages, gender, ZIP codes, genre ratings, and previously chosen movies."¹¹⁰ In late 2009, a few Netflix customers brought a class action lawsuit against the company for privacy violations stemming from the release of their information through the Netflix Prize.¹¹¹ The suit alleged violations of various state and federal privacy laws.¹¹² A few months later, after the FTC became involved, Netflix announced that it had settled the suit and shelved plans for the second contest.¹¹³

104. Internet Movie Database, <http://www.imdb.com> (last visited June 12, 2010).

105. Ideally, the authors would have imported the entire IMDb ratings database to see how many people they could identify in the Netflix data. The authors were afraid, however, that the IMDb terms of service prohibited this. *Netflix Prize Study*, *supra* note 5, at 122. As of Feb. 11, 2009, the IMDb terms of service prohibited, among other things, "data mining, robots, screen scraping, or similar data gathering and extraction tools." Internet Movie Database, IMDb Copyright and Conditions of Use, http://www.imdb.com/help/show_article?conditions (last visited June 12, 2010).

106. IMDb reports that 57 million users visit its site each month. Internet Movie Database, IMDb History, http://www.imdb.com/help/show_leaf/history (last visited June 12, 2010).

107. *Netflix Prize Study*, *supra* note 5, at 123.

108. *Id.*

109. *Id.*

110. Posting of Steve Lohr, *Netflix Awards \$1 Million Prize and Starts a New Contest*, N.Y. TIMES BITS BLOG, <http://bits.blogs.nytimes.com/2009/09/21/netflix-awards-1-million-prize-and-starts-a-new-contest> (Sep. 21, 2009, 10:15 EST).

111. Posting of Ryan Singel, *Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims*, WIRED THREAT LEVEL BLOG, <http://www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit> (Dec. 17, 2009, 16:29 EST).

112. *Id.*

113. Posting of Steve Lohr, *Netflix Cancels Contest Plans and Settles Suit*, N.Y. TIMES BITS BLOG, <http://bits.blogs.nytimes.com/2010/03/12/netflix-cancels-contest-plans-and-settles-suit> (Mar. 12, 2010, 2:46 PM EST).

It seems wise to adopt this aggressively pessimistic assumption of perfect outside information given the avalanche of information now available on the internet¹²³ and, in particular, the rise of blogs and social networks. Never before in human history has it been so easy to peer into the private diaries of so many people.¹²⁴ Alessandro Acquisti and Ralph Gross—researchers who developed an efficient algorithm for using public data to guess people's social security numbers¹²⁵—call this the “age of self-revelation.”¹²⁶

As only one example among many, in early 2009, many Facebook users began posting lists called “25 random things about me.”¹²⁷ The implicit point of the exercise was to bore one's soul—at least a little—by revealing secrets about oneself that friends would not already know.¹²⁸ “25 random things about me” acts like a reidentification virus¹²⁹ because it elicits a vast amount of secret information in a concise, digital format. This is but one example of the rich outside information available on social networking websites. It is no surprise that several researchers have already reidentified people in anonymized social networking data.¹³⁰

c. The Basic Principle: Of Crossed Hands and Inner Joins

One computer security expert summarized the entire field of reidentification to me with a simple motion: He folded his hands together, interleaving his fingers, like a parishioner about to pray. This simple mental image nicely summarizes the basic reidentification operation. If you imagine that your left hand is anonymized data, your right hand is outside information, and your interleaved fingers are places where information from the left matches the right, this image basically captures how reidentification is achieved.

123. See Lakshmanan & Ng, *supra* note 46, at 13:1 (“The assumption that there is no partial [outside] information out there is simply unrealistic in this Internet era.”)

124. Cf. *De-Anonymizing Social Networks*, *supra* note 117, at 17:1–74 (describing sharing of information obtained from social networks)

125. Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 NAT'L ACADEM. SCI. 10975 (2009)

126. Acquisti & Gross, *supra* note 54

127. Douglas Quenqua, *Ah, Yes, More About Me? Here are '25 Random Things'*, N.Y. TIMES, Feb. 4, 2009, at E6

128. See *id.*

129. E.g., Michael Kruse, *25 Random Things About Me to Keep You Caring*, ST. PETERSBURG TIMES, Feb. 23, 2009, available at <http://www.tampabay.com/features/humaninterest/article978293.ece>.

130. *De-Anonymizing Social Networks*, *supra* note 117, at 177; see also Lars Backstrom, Cynthia Dwork & Jon Kleinberg, *Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography*, in 46TH INT'L WORLD WIDE WEB CONFERENCE PROC. 181 (2007), available at <http://portal.acm.org/citation.cfm?id=1242598>.

Database administrators call the hand-folding operation an "inner join."¹³¹ An inner join is an operation combining two database tables, connecting rows from one to rows from the other by matching shared information.¹³² When the rows in the tables represent people, an inner join assumes that rows in which critical fields match refer to the same person, and can be combined into one row in the output table.¹³³ For example, if an adversary has one table that looks like this:

TABLE 5: Anonymized Database

| Race | Birth Date | Sex | ZIP Code | Complaint |
|-------|------------|--------|----------|-----------------|
| Black | 9/20/1965 | Male | 02141 | Short of breath |
| Black | 2/14/1965 | Male | 02141 | Chest pain |
| Black | 10/23/1965 | Female | 02138 | Painful eye |
| Black | 8/24/1965 | Female | 02138 | Wheezing |
| Black | 11/7/1964 | Female | 02138 | Aching joints |
| Black | 12/1/1964 | Female | 02138 | Chest pain |
| White | 10/23/1964 | Male | 02138 | Short of breath |
| White | 3/15/1965 | Female | 02139 | Hypertension |
| White | 8/13/1964 | Male | 02139 | Aching joints |
| White | 5/5/1964 | Male | 02139 | Fever |
| White | 2/13/1967 | Male | 02138 | Vomiting |
| White | 3/21/1967 | Male | 02138 | Back pain |

131. Indeed, in common database systems "INNER JOIN" is the command used to perform such an operation. See, e.g., ALAN BEAULIEU, *LEARNING SQL* 77 (2005); ANDY OITEL & ROBERT SHELDON, *SQL: A BEGINNER'S GUIDE* 264 (2009); ALLEN G. TAYLOR, *SQL ALL-IN-ONE DESK REFERENCE FOR DUMMIES* 309 (2007); PAUL WILTON & JOHN COLBY, *BEGINNING SQL* 90-93 (2005).

132. See BEAULIEU, *supra* note 131.

133. See *id.* This simple example necessarily masks some complexity. For example, reidentifiers must contend with noisy data—errors that cause false positives and false negatives in the inner join. They use probability theory to spot both of these kinds of errors. See *Netflix Prize Study*, *supra* note 5, at 120.

2. Reidentification Techniques

How did Sweeney discover William Weld's diagnoses? How did Barbaro and Zeller find Thelma Arnold? How did Narayanan and Shmatikov reidentify the people in the Netflix Prize dataset? Each researcher combined two sets of data—each of which provided partial answers to the question “who does this data describe?”—and discovered that the combined data answered (or nearly answered) the question.

Even though administrators had removed any data fields they thought might uniquely identify individuals, researchers in each of the three cases unlocked identity by discovering pockets of surprising uniqueness remaining in the data. Just as human fingerprints left at a crime scene can uniquely identify a single person and link that person with “anonymous” information, so too do data subjects generate “data fingerprints”—combinations of values of data shared by nobody else in their table.¹¹⁴

Of course, researchers have long understood the basic intuition behind a data fingerprint; this intuition lay at the heart of endless debates about personally identifiable information (PII). What has startled observers about the new results, however, is that researchers have found data fingerprints in non-PII data, with much greater ease than most would have predicted. It is this element of surprise that has so disrupted the status quo. Sweeney realized the surprising uniqueness of ZIP codes, birth dates, and sex in the U.S. population; Barbaro and Zeller relied upon the uniqueness of a person's search queries; and Narayanan and Shmatikov unearthed the surprising uniqueness of the set of movies a person had seen and rated. These results suggest that maybe everything is PII to one who has access to the right outside information. Although many of the details and formal proofs of this work are beyond the scope of this Article, consider a few aspects of the science that are relevant to law and policy.

a. The Adversary

Computer scientists model anonymization and reidentification as an adversarial game, with anonymization simply an opening move.¹¹⁵ They call the

114. See BBN Tech., *Anonymization & Deidentification*, <http://www.bbn.com/technology/biz/security/axon> (last visited June 12, 2010) (referring to services to remove “fingerprints” in the data”).

115. See Itai Dinur & Kobbi Nissim, *Revealing Information While Preserving Privacy*, in *PROC. 22ND ACM SYMP. ON PRINCIPLES DATABASES SYS.* 202, 203 (2003), available at <http://portal.acm.org/citation.cfm?id=773173>.

person trying to reidentify the data the "adversary."¹¹⁶ They seem not to moralize the adversary, making no assumptions about whether he or she wants to reidentify for good or ill. The defining feature of the adversary seems to be that he or she is, no surprise, adversarial—motivated to do something the data administrator wishes not to happen.

Who are these potential adversaries who might have a motive to reidentify? Narayanan and Shmatikov suggest "stalkers, investigators, nosy colleagues, employers, or neighbors."¹¹⁷ To this list we can add the police, national security analysts, advertisers, and anyone else interested in associating individuals with data.

b. Outside Information

Once an adversary finds a unique data fingerprint, he can link that data to outside information, sometimes called auxiliary information.¹¹⁸ Many anonymization techniques would be perfect, if only the adversary knew nothing else about people in the world. In reality, of course, the world is a wash in data about people, with new databases created every day. Adversaries combine anonymized data with outside information to pry out obscured identities.

Computer scientists make one appropriately conservative assumption about outside information that regulators should adopt: We cannot predict the type and amount of outside information the adversary can access.¹¹⁹ It is naïve to assume that the adversary will be unable to find the particular piece of data needed to unlock anonymized data.¹²⁰ In computer security, this discredited attitude is called "security through obscurity."¹²¹ Not only do reidentification scientists spurn security through obscurity, but they often assume that the adversary possesses the exact piece of data—if it exists—needed to unlock anonymized identities, in order to design responses that protect identity even in this worst case.¹²²

116. *Id.*

117. Arvind Narayanan & Vitaly Shmatikov, *De-Anonymizing Social Networks*, in *PROCC. 2009 30TH IEEE SYMP. ON SECURITY & PRIVACY* 173, 203 [hereinafter *De-Anonymizing Social Networks*] (for a draft version of this article that includes unpublished appendices, see Narayanan & Shmatikov, *infra* note 169).

118. See *Neflix Prize Study*, *supra* note 5, at 112.

119. *Id.*

120. *Id.*

121. SIMSON GARFINKEL ET AL., *PRACTICAL UNIX AND INTERNET SECURITY* 61 (2003) (describing "[t]he problem with security through obscurity").

122. Cf. Cynthia Dwork, *Differential Privacy*, in *AUTOMATA, LANGUAGES AND PROGRAMMING, 33RD INT'L COLLOQUIUM PROC. PART I* 1, 2 (2006), available at <http://www.springer-link.com/content/383p21xk13841688/fulltext.pdf>.

and a separate table that looks like this:

TABLE 6: Database Including PII

| Name | Birth Date | Sex | ZIP Code | Smoker? |
|--------|------------|--------|----------|---------|
| Daniel | 2/14/1965 | Male | 02141 | Yes |
| Forest | 10/23/1964 | Male | 02138 | Yes |
| Helen | 11/7/1964 | Female | 02138 | No |
| Hilary | 3/15/1965 | Female | 02139 | No |
| Kate | 10/23/1965 | Female | 02138 | No |
| Marion | 8/24/1965 | Female | 02138 | Yes |

and she performs an inner join on the birth date, sex, and ZIP code columns, she would produce this:

TABLE 7: Inner Join of Tables 5 and 6 on Birth Date/ZIP/Sex

| Name | Race | Birth Date | Sex | ZIP Code | Complaint | Smoker? |
|--------|-------|------------|--------|----------|-----------------|---------|
| Daniel | Black | 2/14/1965 | Male | 02141 | Chest pain | Yes |
| Kate | Black | 10/23/1965 | Female | 02138 | Painful eye | No |
| Marion | Black | 8/24/1965 | Female | 02138 | Wheezing | Yes |
| Helen | Black | 11/7/1964 | Female | 02138 | Aching joints | No |
| Forest | White | 10/23/1964 | Male | 02138 | Short of breath | Yes |
| Hilary | White | 3/15/1965 | Female | 02139 | Hypertension | No |

Notice that with the two joined tables, the sum of the information is greater than the parts. From the first table alone, the adversary did not know that the white male complaining of shortness of breath was Forest, nor did he know that the person was a smoker. From the second table alone, the adversary knew nothing about Forest's visit to the hospital. After the inner join, the adversary knows all of this.

3. Responding to Objections

In the rest of this Article, I draw many lessons from the three stories presented above and use these lessons to call for aggressive regulatory responses to the failure of anonymization. I anticipate, and in some cases I have confronted, several objections to these interpretations and prescriptions that deserve responses.

a. No Harm, No Foul

The three stories above demonstrate well the power of reidentification, but they do not demonstrate how reidentification can be used to harm people. The researchers described are professional journalists or academics and ethical rules and good moral judgment limited the harm they caused. But do not be misled if the results of these studies seem benign. In Part III, I show how the techniques used in these studies can lead to very real harm, by assembling chains of inferences connecting individuals to harmful facts.¹³⁴

b. Examples of Bad Anonymization

Several people have expressed the opinion that the three stories I describe highlight only the peril of bad anonymization.¹³⁵ These people have argued that the State of Massachusetts, AOL, and Netflix should have foreseen the vulnerability of their approaches to anonymization.¹³⁶ I have many responses.

First, and most fundamentally, the phrase “bad anonymization” is redundant. At least for forget-and-release methods, computer scientists have documented theoretical limits about the type of privacy that can be achieved, which I describe below.¹³⁷ Although some researchers have developed new techniques that do better than forget-and-release anonymization, these techniques have significant limitations, and I explore both the techniques and limitations below.¹³⁸

Second, the fact that such sophisticated data handlers were responsible for these three data releases belies the idea that these were the mistakes of amateurs. Indeed, Netflix boasted about how it perturbed the Netflix Prize data before it released it to protect privacy.¹³⁹ Likewise, AOL's data release was stewarded by PhDs who seemed aware that they were dealing with sensitive information and approved by high-ranking officials.¹⁴⁰ With hindsight it is easy to argue that these breaches were foreseeable—nobody questions anymore

134. See *infra* Part III.A (describing “the database of ruin”).

135. E.g., Khaled El Emam, *Has There Been a Failure of Anonymization?*, ELECTRONIC HEALTH INFORMATION & PRIVACY, Aug. 11, 2009, <http://ehip.blogs.com/ehip/2009/08/has-there-been-a-failure-of-anonymization.html> (“Ohm has taken examples of poorly de-identified datasets that were re-identified and drew broad conclusions from those.”)

136. *Id.*

137. See *infra* Part III.B.1.

138. See *infra* Part III.B.2 and III.B.3.

139. Netflix Prize: FAQ, *supra* note 92 (“Even if, for example, you knew all your own ratings and their dates you probably couldn’t identify them reliably in the data because only a small sample was included (less than one-tenth of our complete dataset) and that data was subject to perturbation.”)

140. Zeller, Jr., *supra* note 78.

whether search queries can be used to identify users—but the past failure of foresight by sophisticated data handlers should give us pause about present claims of bad anonymization.

Third, when one considers the mistakes that have been made by sophisticated data handlers, one can begin to imagine the mistakes being made by the legions of less-sophisticated data handlers, the thousands of IT professionals with no special training in anonymization who are responsible for anonymizing millions of corporate databases. Even if we can divide anonymization cases into good and bad piles, it is safe to assume that the bad towers over the good.

Finally, even if we could teach every data handler in the world how to avoid the mistakes of the past—a daunting and expensive proposition—our new, responsible approach to anonymization would still do nothing to protect all of the data anonymized in the past. Database owners could reanonymize databases they still controlled, but they would not be able to secure the data they shared or redistributed in the past.

c. The Problem of Public Release

It would also be a mistake to conclude that the three stories demonstrate only the peril of public release of anonymized data. Some might argue that had the State of Massachusetts, AOL and Netflix kept their anonymized data to themselves, or at least shared the data much less widely, we would not have had to worry about data privacy.

There is obviously some logic to this objection. In Part IV, I argue that regulators should treat publicly released data differently than privately used data.¹⁴¹

On the other hand, we should not be surprised that we learned the lessons of reidentification only after public releases of data. Reidentification researchers can only reidentify that which they can access. But other people with access to less-public information might be reidentifying in private, keeping the results to themselves. Any time data is shared between two private parties, we should worry about the possibility of reidentification.

Moreover, we must not forget that anonymization is also used by companies as an internal privacy control—to allow Department A to share data with Department B without breaching customer privacy.¹⁴² Just because data is kept wholly within a company does not put to rest concerns about expectations

141. *Infra* Part IV C 1.

142. See *supra* notes 16–17 and accompanying text.

of privacy. If a company promises, for example, to share behavioral data with its marketing arm only in anonymized form, we should worry that the power of easy reidentification gives the company the tools needed to break that promise.

d The Myth of the Superuser

Finally, some might object that the fact that reidentification is possible does not necessarily make it likely to happen. In particular, if there are no motivated, skilled adversaries, then there is no threat. I am particularly sensitive to this objection, because I have criticized those who try to influence policy by exploiting fears of great power, a tactic that relies on what I have called the "Myth of the Superuser."¹⁴³

The power of reidentification, however, is not a Myth of the Superuser story for three reasons: First, reidentification techniques are not Superuser techniques. The Netflix study reveals that it is startlingly easy to reidentify people in anonymized data.¹⁴⁴ Although the average computer user cannot perform an inner join, most people who have taken a course in database management or worked in IT can probably replicate this research using a fast computer and widely available software like Microsoft Excel or Access.¹⁴⁵ Second, the AOL release reminds us about the power of a small group of bored bloggers. And third, there are great financial motivations pushing people to reidentify.¹⁴⁶

Moreover, I did not claim that feats of great power never happen online. Such a conclusion is provably false. Instead, I argued that because it is so easy to exaggerate power, we should hold those offering stories about online power to try to influence policy to a high standard of proof.¹⁴⁷ I concede that my claim of reidentification power should be held to the high standard of proof, and I argue that I have met that standard.

143. See generally Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327 (2008).

144. *Netflix Prize Study*, *supra* note 5, at 112.

145. The INNER JOIN command is taught in beginner database texts. See, e.g., OPPEL & SHELTON, *supra* note 131; TAYLOR, *supra* note 131, at 309; WILSON & COLBY, *supra* note 131, at 501.

146. See Salvador Ochoa et al., *Reidentification of Individuals in Chicago's Homicide Database: A Technical Legal Study* (unpublished student paper) (2001), available at <http://web.mit.edu/sem083/www/assignments/reidentification.html> (discussing financial motives pressing people to reidentify including those affecting marketers and blackmailers).

147. See Ohm, *supra* note 143, at 1402.

4. The Intuition Gap

What each of the foregoing objections highlights is the gap in intuition that persists among privacy experts. These privacy experts, primarily lawyers and business executives charged with protecting their companies' users, clients, and customers, cling to the idea that although anonymization may be weaker than we assumed, it has not failed. They may concede the need to change privacy policies or invest a bit more heavily in technology and expertise in response to the studies cited above, but they hope they need only small tweaks like these and not overhauls.

In the meantime, I predict that computer scientists and talented amateurs will continue to release new examples of powerful reidentification, with each announcement shaking those who still cling to false faiths. As have the past announcements, these future announcements will surprise experts by how cheaply, quickly, and easily supposedly robust anonymization will fall. I make these predictions confidently, because the power of reidentification traces two curves, both moving upward incessantly: the power of computer hardware and the richness of outside information.

The future of anonymization and reidentification thus promises years of awkward transition, as the privacy experts on the wrong side of the intuition gap weaken and then finally abandon their faith in anonymization. It may take years—maybe five, maybe more—before most privacy experts accept that they should abandon faith in anonymization, and these will be years filled with dashed hopes and recalibrated expectations. The gap will probably take longer to close than it truly should, as companies and other interests vested in the cheap, easy promises of anonymization will try to convince others to persist in their faith despite the evidence.

The rest of this Article will mostly skip past the coming, painful years of transition while the intuition gap closes. Instead, it will plan for what happens next, after the intuition gap closes, once we realize that anonymization has failed. What does the failure of anonymization mean for privacy law?

II. HOW THE FAILURE OF ANONYMIZATION DISRUPTS PRIVACY LAW

Policymakers cannot simply ignore easy reidentification, because for decades they enacted laws and regulations while laboring under the robust anonymization assumption. They must now reexamine every privacy law and regulation to see if the easy reidentification result has thwarted their original designs.

Modern privacy laws tend to act preventatively, squeezing down the flow of particular kinds of information in order to reduce predictable risks of harm. In order to squeeze but not cut off valuable transfers of information, legislators have long relied on robust anonymization to deliver the best of both worlds: the benefits of information flow and strong assurances of privacy. The failure of anonymization has exposed this reliance as misguided, throwing carefully balanced statutes out of equilibrium.

At the very least, legislators must abandon the idea that we protect privacy when we do nothing more than identify and remove PII. The idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned.

A. The Evolution of Privacy Law

In the past century, the regulation of privacy in the United States and Europe has evolved from scholarly discussion, to limited common law torts, to broad statutory schemes. Before deciding how to respond to the rise of easy reidentification, we must recognize three themes from this history of privacy law. First, while privacy torts focus solely on compensating injured victims of privacy harms, more recent privacy statutes shift the focus from post hoc redress to problem prevention. Second, this shift has led to the hunt for PII through quasi-scientific exercises in information categorization. Third, legislatures have tried to inject balance into privacy statutes, often by relying on robust anonymization.

1. The Privacy Torts: Compensation for Harm

Most legal scholars point to a celebrated nineteenth-century law review article by Samuel Warren and Louis Brandeis, *The Right to Privacy*,¹⁴⁸ as the wellspring of information privacy law. In the article, Warren and Brandeis, alarmed by the rise of tabloid journalism, advocated a new right of privacy, urging courts to allow plaintiffs to bring new privacy torts.¹⁴⁹ The concept of harm—intangible, incorporeal harm to mere feelings, but harm all the same—loomed large in the article. For example, Warren and Brandeis describe victims of privacy deprivations as experiencing “mental suffering,”¹⁵⁰ “mental pain and distress, far greater than could be inflicted by mere bodily

148 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

149 Irwin R. Krametz, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CALIF. U.L. REV. 703, 709 (1990).

150 Warren & Brandeis, *supra* note 148, at 213.

injury,"¹⁵¹ and "injury to the feelings."¹⁵² That the authors focused on harm is unsurprising because the entire article is a call for "[a]n action of tort for damages in all cases."¹⁵³

Seventy years later, William Prosser synthesized the case law inspired by Warren and Brandeis into the four privacy torts commonly recognized in U.S. jurisdictions today: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, (2) public disclosure of embarrassing private facts about the plaintiff, (3) publicity that places the plaintiff in a false light in the public eye, and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.¹⁵⁴ All four require actual injury, as do all torts.¹⁵⁵

2. Shift to Broad Statutory Privacy: From Harm to Prevention and PII

Courts took the lead during the evolution of the privacy torts¹⁵⁶ while legislatures stayed mostly in the background, doing little more than occasionally codifying privacy torts.¹⁵⁷ Then, about forty years ago, legislatures began to move to the forefront of privacy regulation, enacting sweeping new statutory privacy protections. The fear of computerization motivated this shift.

In the 1960s, the U.S. government began computerizing records about its citizens, combining this data into massive databases. These actions sparked great privacy concerns.¹⁵⁸ Throughout the decade, commentators described threats to privacy from computerization and helped defeat several government proposals.¹⁵⁹ Spurred by this, in 1973 an advisory committee created by the secretary of health, education, and welfare issued a report that proposed a new framework called "Fair Information Principles" (FIPS).¹⁶⁰ The FIPS have

151. *Id.* at 196.

152. *Id.* at 197.

153. *Id.* at 219.

154. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). Prosser was also the reporter for the second Restatement of Torts, in which he also promulgated his four privacy torts. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

155. W. PAGE KEETON ET AL., PROSSER & KEETON ON TORTS 5 (5th ed. 1964) (defining torts as "a body of law which is directed toward the compensation of individuals . . . for losses which they have suffered").

156. Prosser, *supra* note 154, at 386-89.

157. E.g., N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 2007).

158. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 82 (1995).

159. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 506-07 & nn.138-45 (2006).

160. U.S. DEPT. OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

been enormously influential, inspiring statutes,¹⁶¹ law review articles,¹⁶² and multiple refinements.¹⁶³

FIPS require a data protection scheme that provides, among other things, notice and consent, access, data integrity, enforcement, and remedies,¹⁶⁴ but for the present discussion, what the FIPS say is less important than what the FIPS wrought: a very different approach to privacy law, one that embraces rights of privacy that do more than solely redress past harm. Influenced by the FIPS, legislatures have enacted statutes designed to avoid "privacy problems" that have nothing to do with the "injury to feelings" at the heart of the privacy torts. As Dan Solove puts it, "These problems are more structural in nature . . . They involve less the overt insult or reputational harm to a person and more the creation of the risk that a person might be harmed in the future."¹⁶⁵

Thus, beginning in the 1970s, Congress began to enact statutes designed to reduce the risk of harm. Congress's approach for crafting these laws is best described as Linnacan. After first identifying a problem—"a risk that a person might be harmed in the future"¹⁶⁶—lawmakers try to enumerate and categorize types of information that contribute to the risk. They categorize on a macro level (distinguishing between health information, education information, and financial information) and on a micro level (distinguishing between names, account numbers, and other specific data fields). Through this process, they have filled many pages of the U.S. Code with taxonomies of information types that deserve special treatment because of their unusual tendency to cause harm.¹⁶⁷

Congress has thus embraced a wholly data-centric approach, the PII approach, to protecting privacy. This approach assumes that lawmakers can evaluate the inherent riskiness of data categories, assessing with mathematical precision whether or not a particular data field contributes to the problem enough to be regulated. In doing so, it tends to ignore messier, human factors

161. E.g., The Privacy Act of 1974 "requires agencies to follow the Fair Information Practices when gathering and handling personal data." Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U.ILL. L. REV. 357, 361 (citing 5 U.S.C. § 552a(c) (2000)).

162. E.g., Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1; Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 906–22 pt. I (2009).

163. ORGANISATION FOR ECONOMIC COOPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2001), available at <http://www.uhoh.org/oecd-privacy-personal-data.PDF>; Federal Trade Commission, *Fair Information Practice Principles*, <http://www.ftc.gov/ftports/privacy3/fairinfo.shtml> (last visited June 12, 2010).

164. Federal Trade Commission, *supra* note 163.

165. Solove, *supra* note 159, at 487–88.

166. *Id.*

167. See *infra* notes 203–207 (giving examples of statutes that list categories of information).

that should also factor into a risk assessment, such as the likelihood that someone will be motivated enough to care about a particular dataset.¹⁶⁸

It is necessary, however, to distinguish between two very different legislative motivations for singling out categories of information. The easy reidentification result calls into question only the second of these motivations. First, some statutes restrict sensitive information, the kind of information that causes fully-realized harm when disclosed.¹⁶⁹ For example, the Driver's Privacy Protection Act (DPPA) singles out "highly restricted personal information," including sensitive categories like "photograph" and "medical or disability information."¹⁷⁰ Easy reidentification has not disrupted the logic of provisions like this one. Even though robust anonymization has failed, it still makes sense to treat specially those kinds of information that can be used directly to cause harm.

In contrast, lawmakers often single out categories of data for special treatment under the mistaken belief that these categories (and only these) increase the linkability of anonymized data. For instance, the DPPA singles out a second category of personal information, including linkable data fields like social security number and driver identification number, for special, but less restrictive, treatment.¹⁷¹ The law implicitly assumes that this list includes every data field that can link database records to identity—but easy reidentification proves otherwise. When legislators focus on linkability and identifiability in this way, they enshrine release-and-forget, deidentification, and PII-removal approaches to anonymization into law. This approach to legislation makes little sense in light of the advances in easy reidentification.

3. How Legislatures Have Used Anonymization to Balance Interests

Writing about the privacy torts, William Prosser said that "[i]n determining where to draw the line the courts have been invited to exercise nothing less than a power of censorship over what the public may be permitted to read."¹⁷² So too is every privacy statute an "exercise [in] the power of censorship."¹⁷³ These laws restrict the free flow of information. This should give lawmakers

168. See *infra* Part IV B (discussing motive).

169. Arvind Narayanan & Vitaly Shmatikov, *De-Anonymizing Social Networks*, http://userweb.cs.utexas.edu/~shmat/shmat_oak09.pdf, app. B (last visited June 12, 2010) (noting that some laws single out information that "itself is sensitive," while others seek to prevent "deductive disclosure"). This paper was later published without appendices. See *De-Anonymizing Social Networks*, *supra* note 117.

170. 18 USC § 2725(3)-(4) (2000).

171. *Id.*

172. Prosser, *supra* note 154, at 413.

173. *Id.*

great pause. The free flow of information fuels the modern economy, nourishes our hunger for knowledge, shines a light on the inner workings of powerful institutions and organizations, and represents an exercise of liberty.¹⁷⁴ Before enacting any privacy law, lawmakers should weigh the benefits of unfettered information flow against its costs and must calibrate new laws to impose burdens only when they outweigh the harms the laws help avoid.

But for the past forty years, legislators have deployed a perfect, silver bullet solution—anonymization—that has absolved them of the need to engage in overt balancing. Anonymization liberated lawmakers by letting them gloss over the measuring and weighing of countervailing values like security, innovation, and the free flow of information. Regardless of whether those countervailing values weighed heavily, moderately, or barely at all, they would always outweigh the minimized risk to privacy of sharing anonymized data, which lawmakers believed to be almost nil thanks to anonymization. The demise of robust anonymization will throw the statutory legislatures have written out of balance, and lawmakers will need to find a new way to regain balance lost.

Consider how legislatures in two jurisdictions have relied upon anonymization to bring supposed balance to privacy law: the U.S.'s Health Insurance Portability and Accountability Act (HIPAA) and the EU's Data Protection Directive.

a. How HIPAA Used Anonymization to Balance Health Privacy

In 1996, the U.S. Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), hoping to improve healthcare and health insurance in this country.¹⁷⁵ Among the other things it accomplishes, HIPAA is a significant privacy law. Title II of the Act mandates compliance with health privacy regulations, which have been promulgated by the Department

174. See Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN TECH. L. REV. 2, 7–21 (enumerating the benefits of shared information).

175. Pub. L. No. 104-191, 110 Stat. 1936 (1996). According to the preamble to the Act, the purpose of HIPAA is:

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Id.

of Health and Human Services (HHS) and are now known as the HIPAA Privacy Rule.¹⁷⁶

In many ways, the HIPAA Privacy Rule represents the high-water mark for use of PHI to balance privacy risks against valuable uses of information.¹⁷⁷ HIPAA demonstrates Congress's early sensitivity to the power of reidentification, through its treatment of what it calls the "de-identification of health information" (DHI).¹⁷⁸ HIPAA itself exempts data protected by DHI from any regulation whatsoever,¹⁷⁹ but defines DHI so as to allow for further regulatory interpretation—and HHS has used this statutory mandate to define DHI as information that "does not identify an individual" nor provide "a reasonable basis to believe that the information can be used to identify an individual."¹⁸⁰

HHS's Privacy Rule elaborates this vague reasonability standard further in two alternate ways. First, under the so-called "statistical standard," data is DHI if a statistician or other "person with appropriate knowledge . . . and experience" formally determines that the data is not individually identifiable.¹⁸¹ Second, data is DHI under the so-called "safe harbor standard" if the covered entity suppresses or generalizes eighteen enumerated identifiers.¹⁸² The Privacy Rule's list is seemingly exhaustive—perhaps the longest such list in any privacy regulation in the world. Owing to the release of Dr. Sweeney's study around the same time, the Privacy Rule requires the researcher to generalize birth dates to years¹⁸³ and ZIP codes to their initial three digits.¹⁸⁴

Congress and HHS concluded simply that by making data unidentifiable, health professionals could trade sensitive information without impinging on patient privacy. Moreover, they froze these conclusions in amber, enumerating a single, static list, one they concluded would protect privacy in all health privacy contexts.¹⁸⁵ In promulgating the Privacy Rule, regulators relied on their

176 *Id.* § 264 (directing the secretary of Health and Human Services to submit standards for protecting privacy); HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 (2009).

177 Jay Cline, *Privacy Matters: When Is Personal Data Truly De-Identified?*, COMPUTERWORLD, July 24, 2009, http://www.computerworld.com/article/0135898/Privacy_matters_When_is_personal_data_truly_de_identified ("No other country has developed a more rigorous or detailed guidance for how to convert personal data covered by privacy regulations into non-personal data."). HIPAA is not the most recent information privacy law enacted in the U.S. See, e.g., Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, (codified as 15 U.S.C. §§ 6801–6809 (2006)), Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, (codified as 15 U.S.C. §§ 6501–6506 (2006)).

178. See 45 C.F.R. §§ 164.502(d)(2), 164.514(a), (b) (2009).

179. *Id.*

180. *Id.* § 164.514(a).

181. *Id.* § 164.514(b)(1).

182. *Id.* § 164.514(b)(2).

183. *Id.* § 164.514(b)(2)(C).

184. *Id.* § 164.514(b)(2)(B) (allowing only two digits for ZIP codes with 20,000 or fewer residents).

185. Since promulgating the safe harbor list almost a decade ago, HHS has never amended it.

faith in the power of anonymization as a stand-in for a meaningful cost-benefit balancing. This is an opportunity lost, because it is hard to imagine another privacy problem with such starkly presented benefits and costs. On one hand, free exchange of information among medical researchers can help them develop treatments to ease human suffering and save lives. On the other hand, medical secrets are among the most sensitive we hold. It would have been quite instructive to see regulators explicitly weigh such stark choices.

By enumerating eighteen identifiers, the Privacy Rule assumes that any other information that might be contained in a health record can not be used to reidentify. We now understand the flaw in this reasoning, and we should consider revising the Privacy Rule as a result.¹⁸⁶

b How the EU Data Protection Directive Used Anonymization to Balance Internet Privacy

EU lawmakers have also relied upon the power of anonymization to avoid difficult balancing questions. Unlike the American approach with HIPAA, however, the EU enacted a broad industry-spanning law,¹⁸⁷ the Data Protection Directive, which purports to cover any "personal data" held by any data administrator.¹⁸⁸ Data is personal data if it can be used to identify someone "directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."¹⁸⁹

The EU never intended the Directive to apply to all data. Instead, it meant for "personal data" to exclude at least some data—data that was not "directly or indirectly" identifiable, such as anonymized data—from regulation. Like their U.S. counterparts, EU lawmakers imagined they could strike a balance through the power of technology. If anonymization worked, data administrators could freely share information so long as data subjects were no longer "directly or indirectly" identifiable. With this provision, EU lawmakers sought to preserve space in society for the storage and transfer of anonymized data, thereby providing room for unencumbered innovation and free expression.

186. See *infra* Part IV.D.1.

187. The Directive obligates EU countries to transpose its rules into domestic laws within a set time frame. Eur. Comm'n Justice & Home Affairs, *Transposition of the Data Protection Directive*, http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm (last visited June 12, 2010).

188. EU Data Protection Directive *supra* note 1, art. 2(a).

189. *Id.*

Whether and to what extent the Directive retains such a preserve has been debated in the internet privacy context.¹⁹⁰ For several years, the EU has clashed with companies like Google, Yahoo, and Microsoft over what they must do to protect databases that track what their users do online.¹⁹¹ Much of this debate has turned on what companies must do with stored IP addresses. An IP address is a numeric identifier assigned to every computer on the internet.¹⁹² Just as a social security number identifies a person, an IP address identifies a computer, so an IP address can tie online conduct to location and identity.¹⁹³ Every computer reveals its IP address to every other computer it contacts,¹⁹⁴ so every time I visit Google, my computer reveals its IP address to a Google computer.¹⁹⁵ Following longstanding industry practice, Google records my IP address along with details about what I am doing when using Google's services.¹⁹⁶

Google has argued to the EU that it protects the privacy of its users using anonymization, by throwing away part, not all, of every IP address.¹⁹⁷ Specifically, an IP address is composed of four equal pieces called octets,¹⁹⁸ and Google stores the first three octets and deletes the last, claiming that this practice protects user privacy sufficiently.¹⁹⁹ Google's competitors, Microsoft and Yahoo, are much more thorough, throwing away entire IP addresses.²⁰⁰

At its core, this too is a debate about balance—between the wonderful innovations Google promises it can deliver by studying our behavior,²⁰¹ and the

190. See, e.g., Frederick Loh, Note, *Are IP Addresses "Personally Identifiable Information"?*, 41 *S. J.L. & POL'Y FOR INFO. SOC'Y* 681 (2006).

191. E.g., Posting of Sam Hansell, *Europe: Your IP Address Is Personal*, N.Y. TIMES BITS BLOG, <http://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/> (Jan. 22, 2008).

192. DOUGLAS COMER, *INTERNETWORKING WITH TCP/IP* 42 (5th ed. 2006).

193. *Id.* at 43–44.

194. *Id.* at 35–36.

195. *Id.*

196. SIMSON GARTINKEL & GENE SPATFORD, *WEB SECURITY, PRIVACY, AND COMMERCE* 211 (2002).

197. Letter From Google to Congressman Joe Barton 11–15 (Dec. 21, 2007), available at <http://searchengineland.com/pdfs/071222-barton.pdf>.

198. COMER, *supra* note 192, at 53.

199. Letter From Google to Congressman Joe Barton, *supra* note 197, at 14–15.

200. Behavioral Advertising: Industry Practice and Consumers' Expectations, Hearings Before the H. Comm. on Energy and Commerce, Subcomm. on Communications, Technology and the Internet and Subcomm. on Commerce, Trade and Consumer Protection, 111th Cong. 1 (2009) (statement of Anne Toth, Head of Privacy, Yahoo! Inc.); Posting of Peter Cullen, Chief Privacy Strategist at Microsoft, *Microsoft Privacy & Safety: Microsoft Supports Strong Industry Search Data Anonymization Standards*, MICROSOFT PRIVACY AND SAFETY BLOG, <http://blogs.technet.com/privacyimperative/archive/2008/12/08/microsoft-supports-strong-industry-search-data-anonymization-standards.aspx> (Dec. 8, 2008).

201. In 2008, to try to placate those worried about privacy, Google authored a series of blog posts "about how [they] harness the data [they] collect to improve [their] products and services for [their] users." E.g., Posting of Matt Curtis, Software Engineer, *Using Data to Fight Webspam*, THE OFFICIAL

possible harm to users whose IP addresses are known or revealed. Again, claims that we should trust robust anonymization stand in for nuanced careful cost-benefit balancing arguments. Google promises we can have our cake while it eats it too—by placing our trust in data anonymization.

B. How the Failure of Anonymization Disrupts Privacy Law

In addition to HIPAA and the EU Data Protection Directive, almost every single privacy statute and regulation²⁰² ever written in the U.S. and the EU embraces—implicitly or explicitly, pervasively or only incidentally—the assumption that anonymization protects privacy, most often by extending safe harbors from penalty to those who anonymize their data. At the very least, regulators must reexamine every single privacy law and regulation. The loss of robust anonymization reveals the lurking imbalance in these privacy laws, sometimes shifting in favor of protecting privacy too much and sometimes favouring the flow of information too much.

Easy reidentification makes PII-focused laws like HIPAA underprotective by exposing the arbitrariness of their intricate categorization and line drawing. Although HIPAA treats eighteen categories of information as especially identifying,²⁰³ it excludes from this list data about patient visits—like hospital name, diagnosis, year of visit, patient's age, and the first three digits of ZIP code—that an adversary with rich outside information can use to defeat anonymity.

Many other laws follow the same categorization-and-line-drawing approach. The Driver's Privacy Protection Act requires special handling for "personal information" including, among other things, "social security number, driver identification number, name, address . . . , [and] telephone number,"²⁰⁴ while requiring much less protection of "the 5-digit zip code" and "information on vehicular accidents, driving violations, and driver's status."²⁰⁵ Similarly, the Federal Education Rights and Privacy Act (FERPA) singles out for protection "directory information," including, among other things, "name,

GOOGLE BLOG, <http://googleblog.blogspot.com/2008/06/using-data-to-fight-webs-sin.html> (June 27, 2008, 4:51 EST) (linking to earlier posts in the series).

202 In this Article, I focus on statutes and regulations for several reasons. First, these rules provide a concrete set of texts about which I can make correspondingly concrete observations. Second, American and European approaches to privacy legislation differ somewhat, providing a comparative study. Third, when it comes to dictating how information is collected, analyzed, and disclosed in modern life, no other source of law has the influence of privacy statutes and regulations.

203 45 C.F.R. §§ 164.502(d)(2), 164.514(a), (b) (2009).

204 18 U.S.C. § 2725(3) (2000).

205 *Id.*

address, telephone listing, date and place of birth, [and] major field of study."²⁰⁶ Federal Drug Administration regulations permit the disclosure of "records about an individual" associated with clinical trials "[w]here the names and other identifying information are first deleted."²⁰⁷ These are only a few of many laws that draw lines and make distinctions based on the linkability of information. When viewed in light of the easy reidentification result, these provisions, like HIPAA, seem arbitrary and underprotective.

In contrast, easy reidentification makes laws like the EU Data Protection Directive overbroad—in fact, essentially boundless. Because the Directive turns on whether information is "directly or indirectly" linked to a person,²⁰⁸ each successful reidentification of a supposedly anonymized database extends the regulation to cover that database. As reidentification science advances, it expands the EU Directive like an ideal gas to fit the shape of its container. A law that was meant to have limits is rendered limitless, disrupting the careful legislative balance between privacy and information and extending data-handling requirements to all data in all situations.

Notice that the way the easy reidentification result disrupts the Directive is the mirror image of the way it impacts HIPAA. Easy reidentification makes the protections of HIPAA illusory and underinclusive because it deregulates the handling of types of data that can still be used to reidentify and harm. On the other hand, easy reidentification makes laws like the EU Data Protection Directive boundless and overbroad. We should tolerate neither result because both fail to achieve the balance that was originally at the heart of both types of laws.

Most privacy laws match one of these two forms. Even the few that do not fit neatly into one category or the other often contain terms that are made indeterminate and unpredictable by easy reidentification. As one example, the Stored Communications Act in the U.S. applies to "record[s] or other information pertaining to a subscriber . . . or customer," without specifying what degree of identifiability makes a record "pertain."²⁰⁹ As reidentification science advances, courts will struggle to decide whether anonymized records fall within this definition. The vagueness of provisions like this will invite costly litigation and may result in irrational distinctions between jurisdictions and between laws.

206. 20 U.S.C. § 1232g(a)(5)(A) (2006).

207. 21 C.F.R. § 21.70(a)(3)(i) (2009).

208. EU Data Protection Directive, *supra* note 3, art. 2(a).

209. 18 U.S.C. § 2702(c) (2006).

C. The End of PII

1. Quitting the PII Whack-a-Mole Game

At the very least, we must abandon the pervasively held idea that we can protect privacy by simply removing personally identifiable information (PII). This is now a discredited approach. Even if we continue to follow it in marginal, special cases, we must chart a new course in general.

The trouble is that PII is an ever-expanding category. Ten years ago, almost nobody would have categorized movie ratings and search queries as PII, and as a result, no law or regulation did either.²¹⁰ Today, four years after computer scientists exposed the power of these categories of data to identify, no law or regulation yet treats them as PII.

Maybe four years has not been enough time to give regulators the chance to react. After all, HIPAA's Privacy Rule, which took effect in 2003, does incorporate Dr. Sweeney's research, conducted in the mid 1990s.²¹¹ It expressly recognizes the identifying power of ZIP code, birth date, and sex, and carves out special treatment for those who delete or modify them, along with fifteen other categories of information.²¹² Should this be the model of future privacy law reform—whenever reidentification science finds fields of data with identifying power, should we update our regulations to encompass the new fields? No. This would miss the point entirely.

HIPAA's approach to privacy is like the carnival whack-a-mole game: As soon as you whack one mole, another will pop right up. No matter how effectively regulators follow the latest reidentification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered.²¹³ The list of potential PII will never stop growing until it includes everything.²¹⁴

Consider another reidentification study by Narayanan and Shmatikov.²¹⁵ The researchers have reidentified anonymized users of an online social network based almost solely on the stripped-down graph of connections between

210. The Video Privacy Protection Act, enacted in 1988, protects lists of movies watched not because they are PII, but because they are sensitive. 18 U.S.C. § 2710 (2006). For more on the distinction, see *supra* Part II.A.2.

211. See *supra* Part I.B.1.b (describing Sweeney's research).

212. 45 C.F.R. §§ 164.502(d)(2), 164.514(a)-(b) (2009).

213. See Narayanan & Shmatikov, *supra* note 169 ("While some data elements may be uniquely identifying on their own, a key element can be identifying in combination with others").

214. Cf. *id.*; Dinur & Nissim, *supra* note 115, at 202 ("[T]here usually exist other means of identifying patients, via indirectly identifying attributes stored in the database.")

215. See Narayanan & Shmatikov, *supra* note 169.

people.²¹⁶ By comparing the structure of this graph to the nonanonymized graph of a different social network, they could reidentify many people even ignoring almost all usernames, activity information, photos, and every other single piece of identifying information.²¹⁷

To prove the power of the method, the researchers obtained and anonymized the entire Twitter social graph, reducing it to nameless, identity-free nodes representing people connected to other nodes representing Twitter's "follow" relationships. Next, they compared this mostly deidentified husk of a graph²¹⁸ to public data harvested from the Flickr photo-sharing social-network site. As it happens, tens of thousands of Twitter users are also Flickr users, and the researchers used similarities in the structures of Flickr's "contact" graph and Twitter's "follow" graph to reidentify many of the anonymized Twitter user identities. With this technique, they could reidentify the usernames or full names of one-third of the people who subscribed to both Twitter and Flickr.²¹⁹ Given this result, should we add deidentified husks of social networking graphs—a category of information that is almost certainly unregulated under U.S. law yet shared quite often²²⁰—to the HIPAA Privacy Rule list and to the lists in other PII-focused laws and regulations? Of course not.

Instead, lawmakers and regulators should reevaluate any law or regulation that draws distinctions based solely on whether particular data types can be linked to identity, and should avoid drafting new laws or rules grounded in such a distinction. This is an admittedly disruptive prescription. PII has long served as the center of mass around which the data privacy debate has orbited.²²¹ But although disruptive, this proposal is also necessary. Too often, the only thing that gives us comfort about current data practices is that an administrator has gone through the motions of identifying and deleting PII—and in such cases, we deserve no comfort at all. Rather, from now on we need a new organizing principle, one that refuses to play the PII whack-a-mole game. Anonymization has become "privacy theater";²²² it should no longer be considered to provide meaningful guarantees of privacy.

216. See *De-Anonymizing Social Networks*, *supra* note 117, at 182–85.

217. *Id.* at 184.

218. *Id.* To make their study work, the researchers first had to "seed" their data by identifying 150 people who were users of both Twitter and Flickr. They argue that it would not be very difficult for an adversary to find this much information, and they explain how they can use "opportunistic seeding" to reduce the amount of seed data needed. *Id.* at 181–85.

219. *Id.*

220. *Id.* at 174–75 (surveying examples of how social-network data is shared).

221. See Leslie Ann Reis, *Personally Identifiable Information*, in 2 *ENCYCLOPEDIA OF PRIVACY* 383–85 (William G. Staples ed., 2006).

222. Paul M. Schwartz, *Revealing Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 310–15 (2008) (developing the concept of privacy theater).

2. Abandoning "Anonymize" and "Deidentify"

We must also correct the rhetoric we use in information privacy debates. We are using the wrong terms, and we need to stop. We must abolish the word *anonymize*;²²³ let us simply strike it from our debates. A word that should mean, "try to achieve anonymity" is too often understood to mean "achieve anonymity," among technologists and nontechnologists alike. We need a word that conjures effort, not achievement.

Latanya Sweeney has similarly argued against using forms of the word "anonymous" when they are not literally true.²²⁴ Dr. Sweeney instead uses "deidentify" in her research. As she defines it, "[i]n deidentified data, all explicit identifiers, such as SSN, name, address, and telephone number, are removed, generalized, or replaced with a made-up alternative."²²⁵ Owing to her influence, the HIPAA Privacy Rule explicitly refers to the "de-identification of protected health information."²²⁶

Although "deidentify" carries less connotative baggage than "anonymize," which might make it less likely to confuse, I still find it confusing. "Deidentify" describes release-and-forget anonymization, the kind called seriously into question by advances in reidentification research. Despite this, many treat claims of deidentification as promises of robustness,²²⁷ while in reality, people can deidentify robustly or weakly.²²⁸ Whenever a person uses the unmodified word "deidentified," we should demand details and elaboration.

Better yet, we need a new word for privacy-motivated data manipulation that connotes only effort, not success. I propose "scrub." Unlike "anonymize" or "deidentify," it conjures only effort. One can scrub a little, a lot, not enough,

223. *Anonymize* is a relatively young word. The Oxford English Dictionary traces the first use of the word "anonymized" to 1972 by Sir Alan Marles, the UK's Parliamentary Ombudsman. OXFORD ENGLISH DICTIONARY (Additions Series 1997) ("I now lay before Parliament . . . the full but anonymised texts of . . . reports on individual cases.") According to the OED, the usage of the word is "chiefly for statistical purposes." *Id.*

224. Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J.L. MED. & ETHICS 98, 100 (1997) ("The term *anonymous* implies that the data cannot be manipulated or linked to identify an individual.")

225. *Id.*

226. 45 C.F.R. § 164.514(a) (2019) (defining term).

227. See, e.g., infra Part IV.D.2.a (discussing Google's weak approach to anonymization of search engine log files and how the company treats these practices as robust).

228. For similar reasons, I do not recommend replacing "anonymize" with the parallel construction "pseudonymize." See Christopher Sogiotan, *The Problem of Anonymous Vanity Searches*, 3 I/S: J.L. & POL'Y FOR INFO SOC'Y 299, 300 (2007) ("In an effort to protect user privacy, the records were 'pseudonymized' by replacing each individual customer's account I.D. and computer network address with unique random numbers."). Just as "anonymize" fails to acknowledge reversible scrubbing, "pseudonymize" fails to credit robust scrubbing.

or too much, and when we hear the word, we are not predisposed toward any one choice from the list. Even better, technologists have been using the word scrub for many years.²²⁹ In fact, Dr. Sweeney herself has created a system she calls Scrub for "locating and replacing personally-identifying information in medical records."²³⁰

III. HALF MEASURES AND FALSE STARTS

Focusing on things other than PII is a disruptive and necessary first step, but it is not enough alone to restore the balance between privacy and utility that we once enjoyed. How do we fix the dozens, perhaps hundreds, of laws and regulations that we once believed reflected a finely calibrated balance, but in reality rested on a fundamental misunderstanding of science? Before turning in Part IV, to a new test for restoring the balance lost, let us first consider three solutions that are less disruptive to the status quo but are unfortunately also less likely to restore the balance. Legislators must understand why these three solutions—which they will be tempted to treat as the only necessary responses—are not nearly enough, even in combination, to restore balance to privacy law.

First, lawmakers might be tempted to abandon the preventative move of the past forty years, taking the failure of anonymization as a signal to return to a regime that just compensates harm. Even if such a solution involves an aggressive expansion of harm compensation—with new laws defining new types of harms and increasing resources for enforcement—this is a half measure, a necessary but not sufficient solution. Second, lawmakers might be encouraged to wait for the technologists to save us. Unfortunately, although technologists *will* develop better privacy-protection techniques, they will run up against important theoretical limits. Nothing they devise will share the single-bullet universal power once promised by anonymization, and thus any technical solutions they offer must be backed by regulatory approaches. Finally, some will recommend doing little more than banning reidentification. Such a ban will almost certainly fail.

229. See, e.g., Jeremy Kirk, *Yahoo to Scrub Personal Data After Three Months*, IDG NEWS SERVICE, Dec. 17, 2008, available at http://www.pcworld.com/article/155610/yahoo_to_scrub_personal_data_after_three_months.html (reporting Yahoo!'s decision to "anonymize" its databases of sensitive information ninety days after collection); Tommy Peterson, *Data Scrubbing*, COMPUTERWORLD, Feb. 10, 2003, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=78230>.

230. Latanya Sweeney, *Replacing Personally-Identifying Information in Medical Records, the Scrub System*, in 1996 J. AM. MED. INFORMATICS ASS'N PROC. 333.

A. Strictly Punish Those Who Harm

If reidentification makes it easier for malevolent actors like identity thieves, blackmailers, and unscrupulous advertisers to cause harm, perhaps we need to step up enforcement of pre-existing laws prohibiting identity theft,²³¹ extortion,²³² and unfair marketing practices.²³³ Anything we do to deter those who harm and provide remedies for those harmed is, in light of the increased power of reidentification, imperative. But this is merely a necessary response, not a sufficient one.

Full retreat to a tort-based privacy regime, which would abandon the forty-year preventive turn in privacy law, would be a grave mistake, because without regulation, the easy reidentification result will spark a frightening and unprecedented wave of privacy harm by increasing access to what I call the "database of ruin." The database of ruin exists only in potential: It is the worldwide collection of all of the facts held by third parties that can be used to cause privacy-related harm to almost every member of society. Easy access to the database of ruin flows from what I call the "accretion problem."

1. The Accretion Problem

The accretion problem is this. Once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success. Narayanan and Shmatikov explain that "once any piece of data has been linked to a person's real identity, any association between this data and a virtual identity breaks the anonymity of the latter."²³⁴ This is why we should worry even about reidentification events that seem to expose only non-sensitive information, because they increase the *linkability* of data, and thereby expose people to potential future harm.

Because of the accretion problem, every reidentification event, no matter how seemingly benign, brings people closer to harm. Recall that Narayanan and Shmatikov linked two IMEdb users to records in the Netflix Prize database. To some online observers, this connection seemed nonthreatening and trivial²³⁵ because they did not care if others knew what movies they had rented.

231. E.g., 18 U.S.C. § 1028 (2000); CAL. PENAL CODE § 530.5 (1999); MASS. GEN. LAWS ch. 266, § 37E (2002); N.Y. PENAL LAW §§ 190.77–190.84 (2010).

232. E.g., 18 U.S.C. § 872 (2006) (prohibiting extortion by federal government officials).

233. E.g., 15 U.S.C. § 45 (2006) (FTC provision regulating unfair competition); CAL. BUS. & PROF. CODE §§ 17200–210 (2008).

234. Netflix Prize Study, *supra* note 5, at 119.

235. E.g., Comment of chief-ecle to Netflix Prize forum, <http://www.netflixprize.com/community/>

These people failed to see how connecting IMDb data to Netflix data is a step on the path to significant harm. Had Narayanan and Shmatikov not been restricted by academic ethical standards (not to mention moral compunction), they might have connected people to harm themselves.

The researchers could have treated the connections they made between IMDb usernames and Netflix Prize data as the middle links in chains of inferences spreading in two directions: one toward living, breathing people and the other toward harmful facts. For example, they could have tied the list of movies rated in the Netflix Prize database to a list of movies rated by users on Facebook. I suspect that the fingerprint-like uniqueness of Netflix movie preferences would hold for Facebook movie preferences as well.²³⁶

They could have also easily extended the chain in the other direction by making one reasonable assumption: People tend to reuse usernames at different websites.²³⁷ User john_doe20 on IMDb is likely to be john_doe20 on many other websites as well.²³⁸ Relying on this assumption, the researchers could have linked each living, breathing person revealed through Facebook, through the Netflix Prize data, through IMDb username, to a pseudonymous user at another website. They might have done this with noble intentions. Perhaps they could have unearthed the identity of the person who had savagely harassed people on a message board.²³⁹ Maybe they could have determined who had helped plan an attack on a computer system on a 4chan message board.²⁴⁰ But they also could have revealed identities to evil ends. Perhaps they could have tied identities to the pseudonymous people chatting on a child abuse victims' support website, in order to blackmail, frame, or embarrass them.

viewtopic.php?id=809 (Nov. 28, 2007, 09:04:54) ("I think you can find out more abt a person by typing their name into Google, this Netflix data reverse-engineering doesn't seem to be a bigger threat than that."), Comment of jimmyjor to The Physics arXiv Blog, <http://arxivblog.com/?p=142>, (Feb. 17, 2006) ("Choice of movies also does not tell a whole lot"). See also various comments to the posting *Anonymity of Netflix Prize Dataset Broken*, SLASHDOT, <http://it.slashdot.org/article.pl?sid=07/11/27/1334244&from=rs> (Nov. 27, 2007).

236. Of course, even without the Netflix data release, Narayanan and Shmatikov might have been able to connect some records in the IMDb database directly to Facebook records. But recall that for many users, the Netflix data contains movies not rated in IMDb. I am assuming that for some of the people who use all three services, no direct connection between IMDb and Facebook is possible. Thanks to Jane Yakowitz for this point.

237. Arvind Narayanan, *LeakingHub.com: A De-Anonymization Walkthrough*, 33 BITS OF ENTROPY BLOG, <http://33bits.org/2008/11/12/57> (Nov. 12, 2008) ("Many people use a unique username everywhere . . ."), *De-Anonymizing Social Networks*, *supra* note 117, at 6-7 (relying on fact that users tend to reuse usernames on different social networks).

238. See Narayanan, *supra* note 237.

239. Danielle Keats Citron, *Cyber-Civil Rights*, 89 B.U.L. REV. 61, 71-75 (2009) (discussing harassing comments on the AutoAdmit internet discussion board).

240. Matthias Schwart, *The Trolls Among Us*, N.Y. TIMES MAG., Aug. 3, 2008, at MM24 (describing 4chan).

Imagine a large-scale attack on the pseudonyms used on the social networking site Experience Project, which tries to connect users to people who have had similar life experiences.²⁴¹ If the researchers had access to other, harder-to-obtain, outside information, they could have caused even greater harm. With access to Google's search query log file, they might have learned the diseases people had been recently looking up.²⁴² By connecting the IMCb usernames to Facebook biographies, they might have been able to bypass password recovery mechanisms for their victims' online email and bank accounts, allowing them to steal private communications or embezzle money, just as somebody broke into Sarah Palin's email account by guessing that she had met her husband at "Wasilla High."²⁴³ Other possible mischief is easy to imagine when one considers databases that track criminal histories, tax payments, bankruptcies, sensitive health secrets like HIV status and mental health diagnoses, and more.

2. The Database of Ruin

It is as if reidentification and the accretion problem join the data from all of the databases in the world together into one, giant, database-in-the-sky, an irresistible target for the malevolent. Regulators should care about the threat of harm from reidentification because this database-in-the-sky contains information about all of us.

Almost every person in the developed world can be linked to at least one fact in a computer database that an adversary could use for blackmail, discrimination, harassment, or financial or identity theft. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm. Perhaps it is a fact about past conduct, health, or family shame. For almost every one of us, then, we can assume a hypothetical database of ruin, the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given our worst enemies access to it.

241. Experience Project, About Us, <http://www.experienceproject.com/about.php> (last visited July 5, 2010).

242. See *infra* Part IV.D 2.b (discussing the risk to privacy from access to search query logs).

243. See Posting of Sam Gustin, *Alleged Palin Email Hacker Explains*, PORTFOLIO.COM TECH OBSERVER BLOG, <http://www.portfolio.com/views/blogs/the-tech-observer/2008/07/18/alleged-palín-email-hacker-explains> (Sept. 18, 2008).

3. Entropy: Measuring Inchoate Harm

But even regulators who worry about the database of ruin will probably find it hard to care about the reidentification of people to nonsensitive facts like movie ratings. Until there is completed harm—until the database of ruin is accessed—they will think there is no need to regulate. One way to understand the flaw in this is through the concept of entropy.²⁴⁴

In thermodynamics, entropy measures disorder in a system; in information theory, it tracks the amount of information needed to describe possible outcomes.²⁴⁵ Similarly, in reidentification science, entropy measures how close an adversary is to connecting a given fact to a given individual.²⁴⁶ It describes the length of the inference chains heading in opposite directions, quantifying the remaining uncertainty.

Consider entropy in the children's game, Twenty Questions.²⁴⁷ At the start of a game, the Answerer thinks of a subject the Questioner must discover through yes or no questions. Before any questions have been asked, entropy sits at its maximum because the Answerer can be thinking of any subject in the world. With each question, entropy decreases, as each answer eliminates possibilities. The item is a vegetable; it is smaller than a breadbox; it is not green. The Questioner is like the reidentifier, connecting outside information to the anonymized database, reducing entropic uncertainty about the identity of his target.

Entropy formalizes the accretion problem. We should worry about reidentification attacks that fall short of connecting anonymized data to actual identities, and we should worry about reidentification attacks that do not reveal sensitive information. Even learning a little benign information about a supposedly anonymized target reduces entropy and brings an evil adversary closer to his prey.

Consider one more extended metaphor, which Part IV builds upon to illustrate a prescription.²⁴⁸ Imagine each person alive stands on one side of a long hallway specifically dedicated just for him or her. At the other end of the hallway sits that person's ruinous fact, the secret their adversary could use to cause them great harm. In the hallway between the person and the ruinous

244. Arvind Narayanan, *About 33 Bits*, 33 BITS OF ENTROPY BLOG, <http://33bits.org/about> (Sept. 28, 2008) (explaining the concept of entropy).

245. The concept originated with a seminal paper by Claude Shannon. See C.E. Shannon, *A Mathematical Theory of Communication*, 27 BELL SYS. TECH. J. 379 (1948).

246. Narayanan, *supra* note 244.

247. I am indebted to Anna Karion for the analogy.

248. See *infra* Part IV.A.

fact, imagine a long series of closed, locked doors, each lock requiring a different key, which represent the database fields that must be reconnected or the links in the inferential chain that must be established to connect the person to the fact. Finally, imagine many other people clutching keys to some of the doors. Each person represents a database owner, and the keys the person holds represent the inferences the person can make, using the data they own.

Under the current, now discredited PII approach to privacy regulation, we tend to hold database owners—the people in the middle of the hallway—accountable for protecting privacy only if they happen to hold one of two critical keys. First, if they hold the key that unlocks the first door, the one closest to the data subject, we regulate them. This is the linkability form of PII.²⁴⁹ Second, if they hold the key that unlocks the last door, the one closest to the ruinous fact, we also regulate them. This is the sensitivity form of PII.²⁵⁰ But under our current approach, we tend to immunize all of the database owners whose keys unlock only doors in the middle of the hallway.

4. The Need to Regulate Before Completed Harm

If we fail to regulate reidentification that has not yet ripened into harm, then adversaries can nudge each of us ever closer to the brink of connection to our personal database of ruin. It will take some time before most people become precariously compromised, and whether it will take months, years, or decades is difficult to predict. Because some people have more to hide than others, the burden of decreasing entropy will not be distributed equally across society.²⁵¹

Once we are finally connected to our databases of ruin, we will be unable to untie the bell. As soon as Narayanan and Shmatikov tied an IMDb username to Netflix rental data, they created an inferential link in the chain, and no regulator can break that link. Anybody who wants to can replicate their result by downloading the Netflix Prize data²⁵² and mining the IMDb

249. See *supra* note 169–171 and accompanying text (explaining difference between sensitive and linkable forms of PII).

250. See *id.*

251. There are two classes of people who may escape this fate altogether: those with no secrets and those so disconnected from the grid that databases hold few records about them—including many residents of lesser-developed countries. In our own advanced society, I tend to believe that the numbers of people in these groups are so small that they are like myths—the unicorns and mermaids of information privacy. Ultimately, the size of these groups is a difficult empirical question, but one that is not particularly important. I think most people would agree that large majorities in advanced societies are susceptible to reidentification harms, making privacy regulation an important question for huge parts of the world.

252. Since the competition is now over, the data is no longer publicly available, but it has already been downloaded hundreds of times. *Netflix Prize Study*, *supra* note 5, at 119.

user ratings database. Narayanan and Shmatikov have forever reduced the privacy of the people whose information they connected. The FBI cannot easily order connected databases unconnected, nor can they confiscate every last copy of a particularly harmful database.

If we worry about the entire population being dragged irreversibly to the brink of harm, we must regulate in advance because hoping to regulate after the fact is the same as not regulating at all. So long as our identity is separated from the database of ruin by a high degree of entropy, we can rest easy. But as data is connected to data, and as adversaries whittle down entropy, every one of us will soon be thrust to the brink of ruin.

B. Wait for Technology to Save Us

Regulators may wonder whether the technologists will save us first. If we view parallel advances in reidentification and anonymization as an arms race, even though the reidentifiers have raced ahead for now, perhaps the anonymizers will regain the advantage through some future breakthrough. Maybe such a breakthrough will even restore the status quo and shift the privacy laws back into balance.

We should not expect a major breakthrough for release-and-forget anonymization, because computer scientists have proved theoretical limits of the power of such techniques. The utility and privacy of data are linked, and so long as data is useful, even in the slightest, then it is also potentially reidentifiable. Moreover, for many leading release-and-forget techniques, the tradeoff is not proportional: As the utility of data increases even a little, the privacy plummets.

We might, however, enjoy some help from new technology, although we should not expect a breakthrough. Computer scientists have devised techniques that are much more resistant to reidentification than release-and-forget. Data administrators may use some of these techniques—interactive techniques, aggregation, access controls, and audit trails—to share their data with a reduced risk of reidentification. Alas, despite the promise of these techniques, they cannot match the sweeping privacy promises that once were made regarding release-and-forget anonymization. The improved techniques tend to be much slower, more complex, and more expensive than simple anonymization. Worse, these techniques are useless for many types of data analysis problems. Technological advances like these may provide some relief in a post-anonymization, post-PII world, but they can never replace the need for a regulatory response.

1. Why Not to Expect a Major Breakthrough

Computer scientists have begun to conclude that in the arms race between release-and-forget anonymization and reidentification, the reidentifiers hold the permanent upper hand.

a. Utility and Privacy: Two Concepts at War

Utility and privacy are, at bottom, two goals at war with one another.²⁵³ In order to be useful, anonymized data must be imperfectly anonymous. "[P]erfect privacy can be achieved by publishing nothing at all—but this has no utility; perfect utility can be obtained by publishing the data exactly as received from the respondents, but this offers no privacy."²⁵⁴ No matter what the data administrator does to anonymize the data, an adversary with the right outside information can use the data's residual utility to reveal other information. Thus, at least for useful databases, perfect anonymization is impossible.²⁵⁵ Theorists call this the impossibility result.²⁵⁶ There is always some piece of outside information that could be combined with anonymized data to reveal private information about an individual.²⁵⁷

Cynthia Dwork offers proof of the impossibility result.²⁵⁸ Although useful data can never be perfectly private, it is important to understand the practical limits of this result;²⁵⁹ some kinds of theoretical privacy breach may concern policymakers very little. To use Dwork's example, if a database owner releases an aggregate statistic listing the average heights of women in the world by national origin, an adversary who happens to know that his target is precisely two inches shorter than the average Lithuanian woman may learn a "private" fact by studying the database.²⁶⁰ Although we would properly say that the utility of the anonymized data revealed a private fact when combined with outside information,²⁶¹ we would be foolhardy to regulate or forbid the release of databases containing aggregated height data to avoid this possibility. In

253. Shuchi Chawla et al., *Toward Privacy in Public Databases*, in 2 THEORY CRYPTOGRAPHY CONF. 363 (2005).

254. *Id.* at 364.

255. Dwork, *supra* note 122, at 4.

256. *Id.*

257. Danur S. Nisim, *supra* note 115, at 203 (showing, for a particular model, "tight impossibility results," meaning that privacy would require "totally ruining the database usability").

258. Dwork, *supra* note 122.

259. *Id.*

260. *Id.*

261. *Id.*

this case, the richness of the outside information creates almost all of the privacy breach, and the statistic itself contributes very little.

Although the impossibility result should inform regulation, it does not translate directly into a prescription. It does not lead, for example, to the conclusion that all anonymization techniques are fatally flawed, but instead, as Cynthia Dwork puts, "to a new approach to formulating privacy's goals."²⁶² She calls her preferred goal "differential privacy" and ties it to so-called interactive techniques. Differential privacy and interactive techniques are discussed below.

b. The Inverse and Imbalanced Relationship

Other theoretical work suggests that release-and-forget anonymization techniques are particularly ill-suited for protecting privacy while preserving the utility of data. Professor Shmatikov, one of the Netflix Prize researchers, coauthored a study with Justin Buckell that offers some depressing insights about the tradeoffs between utility and privacy for such techniques. As the researchers put it, "even modest privacy gains require almost complete destruction of the data-mining utility."²⁶³

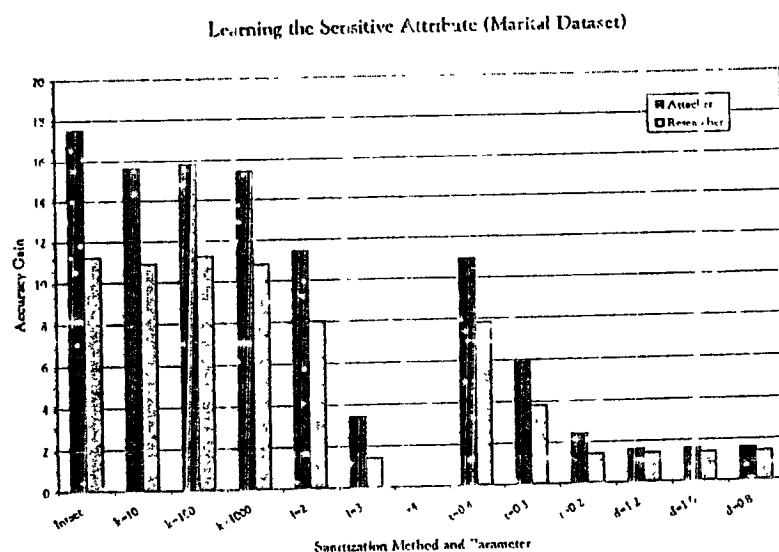
The researchers compared several widely used anonymization techniques to a form of anonymization so extreme no data administrator would ever use it: a completely wiped database with absolutely no information beyond the single field of information under study²⁶⁴—for a health study perhaps the diagnoses, for an education study the grade point averages, and for a labor study the salaries. We would hope that real-world anonymization would compare very favorably to such an extreme method of anonymization, of course supplying worse privacy, but in exchange preserving much better utility.²⁶⁵ Although the full details are beyond the scope of this Article, consider the intuition revealed in the following graph:

262. *Id.*

263. Buckell & Shmatikov, *supra* note 48, at 70, 76.

264. *Id.* at 70–71.

265. *See id.*

FIGURE 1: Effects on Privacy and Utility of Anonymization²⁶⁶

In Figure 1, the pairs of bars represent the same databases transformed into many different forms using widespread anonymization techniques. For each pair, the left, black bar represents the privacy of the data, with smaller bars signifying more privacy. The right, gray bars represent the utility of the data, with longer bars meaning more utility. Anonymization techniques search for ways to shorten the left bar without shortening the right bar too much, and the holy grail of anonymization would be a short, black bar next to a long, gray bar. Even a quick scan of the graph reveals the absence of this condition.

The leftmost pair of bars, with a privacy score of almost eighteen and a utility score of about eleven, represents the original, unadulterated data. A score of zero represents the utility or privacy of completely wiped data. Notice how the first three pairs of bars, the ones labeled with the letter *k*, describe techniques that preserve a lot of utility while improving privacy very little.²⁶⁸

266. This figure has been adapted from a figure in *id.* at 76. Only the formatting has been changed; the substance of the figure remains the same.

268. These bars represent techniques that achieve *k*-anonymity, a widely embraced metric for strong anonymity. *Id.* at 71; Sweeney, *supra* note 8 (defining *k*-anonymity).

Although the second trio of bars, those labeled with the letter l,²⁶⁹ show much greater improvements in privacy than the first trio, such improvements come only at great losses to utility.

These results show that for traditional, widespread, release-and-forget anonymization, not only are privacy and utility related, but their relationship is skewed. Small increases in utility are matched by even bigger decreases in privacy, and small increases in privacy cause large decreases in utility. The researchers concluded that even the most sophisticated anonymization techniques were scarcely better than simply throwing away almost all of the data instead.

Thus, using traditional, release-and-forget, PII-focused anonymization techniques, any data that is even minimally useful can never be perfectly anonymous, and small gains in utility result in greater losses for privacy. Both of these relationships cut against faith in anonymization and in favor of other forms of regulation.

2. The Prospect of Something Better Than Release-and-Forget

Researchers have developed a few techniques that protect privacy much better than the traditional, release-and-forget techniques. These work by relaxing either the release or the forget requirement. For example, some data administrators never release raw data, releasing only aggregated statistics instead. Every day, *USA Today* summarizes a survey in a colorful graph on their front page. Armed only with these survey responses, it would be very difficult for a reidentifier to prove that any particular person took part in a *USA Today* survey, much less gave a particular response.

Similarly, some researchers favor interactive techniques.²⁷⁰ With these techniques, the data administrator answers questions about the data without ever releasing the underlying data. For example, an analyst might ask, what percentage of the people in your database have been diagnosed with this rare form of cancer? This might prompt the administrator to calculate and return the answer—say, 2 percent. In most cases, reidentifiers will find it much more difficult to link answers like these to identity than if they had access to the underlying raw data.

269. These bars represent *l*-diversity, another widely adopted metric. The final six bars represent *t*-closeness. Brickell & Shmatikov, *supra* note 48, at 70–71.

270. Cynthia Dwork et al., *Calibrating Noise to Sensitivity in Private Data Analysis*, in 2006 THEORY OF CRYPTOGRAPHY CONF. 265, 267.

Researchers can do even better. Using one class of interactive techniques, those that satisfy a requirement called differential privacy,²⁷¹ the data administrator never even releases the accurate statistic; instead, she introduces a carefully calculated amount of random noise to the answer, ensuring mathematically that even the most sophisticated reidentifier will not be able to use the answer to unearth information about the people in the database.²⁷²

Finally, just as these techniques refer to something less than full release, other techniques refuse to forget—instead, they monitor what happens to data *after* release. Borrowing from computer security research, these techniques involve the use of access controls and audit trails.²⁷³ Using these techniques, data administrators release their data but only after protecting it using software that limits access and tracks usage. The data analyst who receives the protected data will be able to interact with it only in limited ways, and the analyst's every move will be recorded in the audit trail and reported back to the data administrator or a third-party watchdog.

3. The Limitations of the Improved Techniques

Unfortunately, these alternatives do not make up for the broken promises of release-and-forget anonymization. For starters, they tend to be less flexible than traditional anonymization. Interactive techniques require constant participation from the data administrator. This increases the cost of analysis and reduces the rate of new analysis. Because an analyst must submit requests and wait for responses, he is not free to simply test theory after theory at the maximum rate. Even worse, without access to the raw data, he might miss useful research inquiries that reveal themselves to those who study trends in the data.

Furthermore, even with interactive techniques and aggregation, data administrators cannot promise perfect privacy. As an example, if an adversary somehow knows that his target is the only man who visited a hospital clinic Thursday afternoon, then the aggregated answer to the question, "diagnoses of men who visited the clinic Thursday afternoon" reveals sensitive information tied directly to an identity. As another example, despite decades of denials from the Census Bureau, scholars have unearthed proof that the agency provided aggregated, city-block-level data that helped locate Japanese Americans who were then sent to internment camps during the Second World

271. See Dwork, *supra* note 122, at 8–9.

272. See Adam & Wortmann, *supra* note 60, at 540 (describing the "output-perturbation approach").

273. For more information on access controls in the computer security context, see RICK LEITINEN ET AL., *COMPUTER SECURITY BASICS* 66–77 (2006).

War.²⁷⁴ Even though the data did not identify particular houses or families, just telling authorities how many Japanese lived on each block gave them enough information to do enormous harm.

Interactive techniques that introduce noise are also of limited usefulness. For example, a city may want to analyze census data to determine where to run a bus line to serve elderly residents. Noise introduced to provide privacy may inadvertently produce the wrong answer to this question.²⁷⁵ Similarly, law enforcement data miners may find it unacceptable to tell a judge that they are using a “noisy” technique to justify asking for a search warrant to search a home.²⁷⁶ Techniques that satisfy differential privacy also require complex calculations that can be costly to perform.²⁷⁷

Finally, computer security researchers have thoroughly documented the problem with creating robust access controls.²⁷⁸ Simply put, even the best computer security solutions are bug-prone, as well as being expensive to create and deploy.²⁷⁹ All of these reasons explain why the vast majority of data shared or stored today is protected—if at all—by traditional, release-and-forget anonymization, not by these more exotic, more cumbersome, and more expensive alternatives.

Even if computer scientists tomorrow develop a groundbreaking technique that secures data much more robustly than anything done today—and this is a very unlikely “if”—the new technique will only work on data secured in the future; it will do nothing to protect data that has been stored or disclosed in the past. A database, once released, can become easier to reidentify but never more difficult. Long chains of inferences from past reidentification cannot be broken with tomorrow’s advances.

Techniques that eschew release-and-forget may improve over time, but because of inherent limitations like those described above, they will never supply

274. William Selzer & Margo Anderson, Population Association of America, After Pearl Harbor: The Proper Role of Population Data Systems in Time of War (Mar. 28, 2000) (unpublished paper), available at <http://panthe.file.uwin.edu/margo/www/gov-ratner/paper.pdf>.

275. See Chawla et al., *supra* note 253, at 366.

276. The difficulty of using “noisy” techniques in police work is illustrated by a recent AP story that documents one instance where the addition of “random material” to a database resulted in repeated unnecessary police deployments. Cops’ Computer Glitch Led to Wrong Address, MSNBC NEWS, Mar. 19, 2010, <http://www.msnbc.msn.com/id/35950730>.

277. Jon Kleinberg et al., *Analzing Boolean Attributes*, in 2000 ACM SYMP. ON PRINCIPLES DATABASE SYS. 86 (proving that particular method supporting interactive technique is NP-hard, meaning computationally expensive).

278. BRUCE SCHNIEER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 87–101 (2003).

279. *Id.*; cf. FREDERICK P. BROOKS, JR., THE MYTHICAL MAN-MONTH (1975) (discussing how software engineering principles lead to bugs).

a silver-bullet alternative. Technology cannot save the day, and regulation must play a role.

C. Ban Reidentification

Finally, some have urged simply banning reidentification.²⁸⁰ Lawmakers can offer a straightforward argument for a ban: By anonymizing data, a data administrator gives notice of her intent to protect the privacy of her data subjects, who may rely on this notice when consenting to provide her their data. A reidentifying adversary thwarts this intent and undermines this consent so much that we might need a law banning the act itself.

A reidentification ban is sure to fail, however, because it is impossible to enforce. How do you detect an act of reidentification?²⁸¹ Reidentification can happen completely in the shadows. Imagine that Amazon.com anonymizes its customer purchase database and transmits it to a marketing firm. Imagine further that although the marketing firm promises not to reidentify people in Amazon's database, it could increase profits significantly by doing so. If the marketing firm breaks its promise and reidentifies, how will Amazon or anybody else ever know? The marketing firm can conduct the reidentification in secret, and gains in revenue may not be detectable to the vendor.

This problem appears insurmountable, although four forces might help to ameliorate it. First, lawmakers might pair a ban with stricter penalties and better enforcement, for example by declaring reidentification a felony and providing extra money to the FBI and FTC for enforcement. Second, lawmakers can give citizens a private right of action against those who reidentify.²⁸² Third, lawmakers can mandate software audit trails for those who use anonymized data.²⁸³ Finally, a smaller scale ban, one imposed only on trusted recipients of specific databases—for example, a ban prohibiting government data-miners from reidentifying—may be much easier to enforce.²⁸⁴

280. Earl Lave, *A Question of Identity: Computer-Based Pinpointing of 'Anonymous' Health Records Prompts Calls for Tighter Security*, *NEWSDAY*, Nov. 21, 2000, at C8 (quoting Janfort Goldman, head of the Health Privacy Project at Georgetown University as saying: "Our goal has been to get a national policy making it illegal to re-identify an anonymized database").

281. *Id.* ("As long as the data recipient is discreet, an agency may never learn if its information is being compromised." (citing Larany & Sweeney)).

282. They can model this on the Federal Stored Communications Act, which provides a civil cause of action to any "person aggrieved by any violation" of the Act. 18 U.S.C. § 2707 (2006).

283. *E.g.*, 45 C.F.R. § 164.308(n)(1)(ii)(D) (2009) (describing HIPAA Security Rule mandating "Information system activity review" including regular review of "audit logs").

284. For another example, see *infra* Part IV.D.1 (discussing the ban on reidentification for trusted recipients of health information).

I predict that any of these marginal improvements would still be outweighed by the inherent difficulty of detecting secret reidentification for private gain. This significant detection problem makes a ban extremely unlikely to succeed.

IV. RESTORING BALANCE TO PRIVACY LAW AFTER THE FAILURE OF ANONYMIZATION

Once regulators conclude that the three partial solutions discussed above are not enough to restore balance to privacy law after the failure of anonymization, they must do more. They should weigh the benefits of unfettered information flow against the costs of privacy harms. They should incorporate risk assessment strategies that deal with the reality of easy reidentification as the old PII model never could. Ultimately, they should consider a series of factors to identify situations in which harm is likely and whether it outweighs the benefits of unfettered information flow. When they identify harm that outweighs these benefits, they should regulate, focusing on narrow contexts and specific sectors rather than trying to regulate broadly across industries. To demonstrate how this approach works, this Part ends with two case studies recommending new strategies for regulating the privacy of health and internet usage information.

A. Which Database Owners Should We Regulate Anew?

In the search for a new organizing principle to supplement PII, I start from the premise that any privacy rule we devise must distinguish between different types of database owners and different types of databases. This approach might sound like PII, but it is broader. The problem is not that the PII approach categorizes; the problem is that it focuses on only a few, narrowly drawn categories that seem insufficient and even somewhat arbitrary in light of easy reidentification. Recall the hallway metaphor: PII-based rules regulate only those people with a key to the first door closest to the data subject (those that can link to a user's identity) or a key to the last door closest to the ruinous fact (those holding sensitive information).²⁸⁵ For example, HIPAA singles out for special treatment social security numbers (linkable data) and medical diagnoses (sensitive data). PII rules ignore the people who can unlock doors only in the middle.

285 See text accompanying *supra* notes 248–250.

The power of reidentification demands that we begin to regulate the middle. But how? It would be logically justifiable but overly aggressive to regulate any entity possessing any fragment of data at any point along the chain of inferences, covering even a person holding only one key. We should aim to direct scarce regulatory resources at those database owners that most contribute to the risk of the database of ruin through well-tuned rules. A rule that regulates the database owner in the middle that possesses but a single scrap of unimportant data puts too much regulatory focus on too slight a risk.

Which database owners in the middle most contribute to the risk of harm and thereby most deserve government scrutiny and regulation? To the current PII-approach—regulation for those holding linkable data and those holding sensitive data—I propose we add at least one more category of database owners, the “large entropy reducers.”²⁸⁶ Large entropy reducers are entities that amass massive databases containing so many links between so many disparate kinds of information that they represent a significant part of the database of ruin, even if they delete from their databases a particularly sensitive and directly linkable information.

We can justify treating these entities differently using the language of duty and fault. Because large entropy reducers serve as one-stop shops for adversaries trying to link people to ruinous facts, they owe their data subjects a heightened duty of care. When a large entropy reducer loses control of its massive database, it causes much more harm than an entity holding much less data.

Who are large entropy reducers? In the hallway metaphor, they are the people clutching many keys; imagine the mythical janitor: keyring, jangling with dozens of different keys. In practice, this category includes large credit agencies like Experian, TransUnion, and Equifax; commercial data brokers like ChoicePoint, Acxiom, and LexisNexis; and internet search providers like Google, Microsoft, and Yahoo. These are among the most important large entropy reducers, but there are many others, and we should develop a more precise definition of the category, perhaps one taking advantage of the formal definition of entropy.

286. In addition to large entropy reducers, other classes of database owners probably deserve new regulation to account for the way they increase the risk of harm due to easy reidentification. For one, some database owners can make links between fields of information that can be connected by few other people—they can unlock doors requiring keys held by few people. For example, consider how a cell phone provider or automobile toll booth administrator can track physical movement and location in ways that few other providers can. Likewise, some database owners hold fields of data that act as identifiers on many sites, making them powerful tools for reidentification. Increasingly, email addresses act in this manner, as websites use them in place of usernames. Perhaps any entity holding an email address deserves new regulation. I plan in future work to develop these categories further and to flesh out the arguments for regulating them more closely.

We should expand existing privacy laws and enact new privacy laws that regulate the behavior of companies like these. To be sure, many of these firms are already obligated to comply with many different privacy laws, but in light of easy reidentification and the database of ruin, we need to regulate them more, perhaps with new rules tailored to limiting the type of risk of reidentification such providers represent.

B. Regulatory Principles

Now that we know whom to regulate—database owners holding linkable or sensitive data (PII) and large entropy reducers—we turn to the content of regulation. How should regulators respond to the power of reidentification and the collapse of our faith in anonymization? Before we turn to a list of factors that will guide us to the proper regulation, we need to understand some overarching principles. This step is necessary because so much of how we regulate privacy depends on our faith in anonymization; stripped of this faith, we need to reevaluate some core principles.

1. From Math to Sociology

Regulators need to shift away from thinking about regulation, privacy, and risk only from the point of view of the data, asking whether a particular field of data viewed in a vacuum is identifiable. Instead, regulators must ask a broader set of questions that help reveal the risk of reidentification and threat of harm. They should ask, for example, what has the data administrator done to reduce the risk of reidentification? Who will try to invade the privacy of the people in the data, and are they likely to succeed? Do the history, practices, traditions, and structural features of the industry or sector instill particular confidence or doubt about the likelihood of privacy?

Notice that while the old approach centered almost entirely on technological questions—it was math and statistics all the way down—the new inquiry is cast also in sociological, psychological, and institutional terms. Because easy reidentification has taken away purely technological solutions that worked irrespective of these messier, human considerations, it follows that new solutions must explore, at least in part, the messiness.²⁸⁷

287. See Chawla et al., *supra* note 253, at 367 (noting that the relative advantage of one interactive technique is that "the real data can be deleted or locked in a vault, and so may be less vulnerable to bribery of the database administrator")

2. Support for Both Comprehensive and Contextual Regulation

The failure of anonymization will complicate one of the longest-running debates in information privacy law. Should regulators enact comprehensive, cross-industry privacy reform, or should they instead tailor specific regulations to specific sectors?²⁸⁸ Usually the competing choices are labeled, respectively, the European and United States approaches. In a postanonymization world, neither approach is sufficient alone. We need to focus on particular risks arising from specific sectors because it is difficult to balance interests comprehensively without relying on anonymization. On the other hand, we need a comprehensive regulation that sets a floor of privacy protection because anonymization permits easy access to the database of ruin. In aiming for both general and specific solutions, this recommendation echoes Dan Solove, who cautions that privacy should be addressed neither too specifically nor too generally.²⁸⁹ Solove says that we should simultaneously "resolve privacy issues by looking to the specific context,"²⁹⁰ while at the same time using "a general framework to identify privacy harms or problems and to understand why they are problematic."²⁹¹

Thus, the U.S.'s exclusively sectoral approach is flawed, because it allows entire industries to escape privacy regulation completely based on the illusion that some data, harmless data, data in the middle of long chains of inferences leading to harm, is so bland and nonthreatening that it is not likely to lead to harm if it falls into the wrong hands. The principle of accretive reidentification shatters this illusion. Data almost always forms the middle link in chains of inferences, and any release of data brings us at least a little closer to our personal databases of ruin. For this reason, there is an urgent need for comprehensive privacy reform in this country. A law should mandate a minimum floor of safe data-handling practices on every data handler in the U.S. Further, it should require even stricter data-handling practices for every large entropy reducer in the U.S.

But on the other hand, the European approach—and specifically the approach the EU has taken in the Data Protection Directive—sets the height of this floor too high. Many observers have complained about the onerous

²⁸⁸ See, e.g., Schwartz, *supra* note 162, at 908–16 (discussing history of sectoral and comprehensive approaches to privacy law).

²⁸⁹ DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 46–49 (2008).

²⁹⁰ *Id.* at 48.

²⁹¹ *Id.* at 49.

obligations of the Directive.²⁹² It might have made good sense to impose such strict requirements (notice, consent, disclosure, accountability) on data administrators when we still believed in the power of anonymization because the law left the administrators with a fair choice: Anonymize your data to escape these burdens or keep your data identifiable and comply.

But as we have seen, easy reidentification has mostly taken away this choice, thereby broadening the reach of the Directive considerably. Today, the EU hounds Google about IP addresses; tomorrow, it can make similar arguments about virtually any data-possessing company or industry. A European privacy regulator can reasonably argue that any database containing facts (no matter how well scrubbed) relating to people (no matter how indirectly) very likely now falls within the Directive. It can impose the obligations of the Directive even on those who maintain databases that contain nothing that a layperson would recognize as relating to an individual, so long as the data contains idiosyncratic facts about the lives of individuals.

I suspect that some of those who originally supported the Directive might feel differently about a Directive that essentially provides no exception for scrubbed data—a Directive covering most of the data in society. The Directive's aggressive data-handling obligations might have seemed to strike the proper balance between information flow and privacy when we thought that they were restricted to "personal data," but once reidentification science redefines "personal data" to include almost all data, the obligations of the Directive might seem too burdensome. For these reasons, the European Union might want to reconsider whether it should lower the floor of its comprehensive data-handling obligations.

Finally, once the U.S. tackles comprehensive privacy reform and the EU lowers the burdens of the directive, both governments should expand the process of imposing heightened privacy regulations on particular sectors. What might be needed above the comprehensive floor for health records may not be needed for phone records, and what might solve the problems of private data release probably will not work for public releases.²⁹³ This approach borrows from Helen Nissenbaum, who urges us to understand privacy through what she calls "contextual integrity," which "couches its prescriptions always within the bounds of a given context" as better than other "universal"

292. E.g., DOROTHIL HEISENBERG, *NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES AND PERSONAL DATA PROTECTION* 29, 30 (2005) (calling parts of the Directive "quite strict" and "overly complex and burdensome").

293. Cf. *infra* Part IV.D (discussing specific rules for health privacy and search engine privacy contexts).

accounts.²⁹⁴ This approach also stands in stark contrast to the advice of other information privacy scholars and activists, who tend to valorize sweeping, society-wide approaches to protecting privacy and say nothing complimentary about the U.S.'s sectoral approach.

What easy reidentification thus demands is a combination of comprehensive data-protection regulation and targeted, enhanced obligations for specific sectors. Many others have laid out the persuasive case for a comprehensive data privacy law in the United States, so I refer the reader elsewhere for that topic.²⁹⁵ The rest of the Article explores how to design sector-specific data privacy laws, now that we can no longer lean upon the crutch of robust anonymization to give us balance. What does a post-anonymization privacy law look like?

C. The Test

In the post-anonymization age, once regulators pick a target for regulation—say, large entropy reducers in the healthcare industry—they should weigh the following factors to determine the risk of reidentification in that context. The list is not exhaustive; other factors might be relevant.²⁹⁶ The factors serve two purposes: They are indicators of risk and instruments for reducing risk. As indicators, they signal the likelihood of privacy harm. For example, when data administrators in a given context tend to store massive quantities of information, the risk of reidentification increases. Regulators should use these indicative factors like a score card, tallying up the risk of reidentification.

Once regulators decide to regulate, they should then treat these factors as instruments for reducing risk—the tuning knobs they can tweak through legislation and regulation to reduce the risk of harm. As only one example, regulators might ban public releases of a type of data outright while declining to regulate private uses of data.

294. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 154 (2004).

295. E.g., Solove & Hooftagle, *supra* note 161.

296. The European privacy watchdog, the Article 29 Working Group, offers the following, similar but not identical, list of factors:

The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account. On the other hand [one]... should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed.

2007 Working Party Opinion, *supra* note 28, at 15.

1. Five Factors for Assessing the Risk of Privacy Harm

Data-Handling Techniques

How do different data-handling techniques affect the risks of reidentification? Experts probably cannot answer this question with mathematical precision, it is unlikely we can ever know, say, that the suppression of names and social security numbers produces an 82 percent risk, while interactive techniques satisfying differential privacy produce a 1 percent risk. Still, computer scientists could likely provide a rough relative ordering of different techniques—or at the very least, grade data-handling practices according to whether the risk of reidentification is high, medium, or low.²⁹⁷ For example, computer scientists might grade favorably a database owner that uses the kind of new interactive techniques described earlier, although remember that such techniques are no panacea.

Private Versus Public Release

Regulators should scrutinize data releases to the general public much more closely than they do private releases between trusted parties. We fear the database of ruin because we worry that our worst enemy can access it, but if we use regulation to limit the flow of information to trusted relationships between private parties, we can breathe a little easier. It is no coincidence that every case study presented in Part I.B involved the public release of anonymized data. In each case, the researcher or researchers targeted the particular data because it was easy to get, and in the AOL search query example in particular, an army of blogger-reidentifiers acted as a force multiplier, aggravating greatly the breach and the harm.

My argument against public releases of data pushes back against a tide of theory and sentiment flowing in exactly the opposite direction. Commentators place great stock in the “wisdom of crowds,” the idea that “all of us are smarter than any of us.”²⁹⁸ Companies like Netflix release great stores of information they once held closely to try to harness these masses.²⁹⁹

297. Some computer scientists have already tentatively offered studies that attempt to categorize the risk of reidentification of different techniques. See, e.g., Lakshmanan et al., *supra* note 46 (focusing on anonymization); Adam & Wortmann, *supra* note 60 (evaluating methods, including conceptual, query restriction, data perturbation, and output perturbation). These studies do not take into account the latest advances in reidentification, but they are models for future work.

298. SUROWIECKI, *supra* note 15.

299. See Thompson, *supra* note 93.

The argument even throws some sand into the gears of the Obama Administration's tech-savvy new approach to governance. Through the launch of websites like data.gov³⁰⁰ and the appointment of federal officials like CTO Aneesh Chopra³⁰¹ and CIO Vivek Kundra,³⁰² the administration has promised to release massive databases heralding a twenty-first century mode of government openness.³⁰³ Amidst the accolades that have been showered upon the government for these efforts,³⁰⁴ one should pause to consider the costs. We must remember that utility and privacy are two sides of the same coin,³⁰⁵ and we should assume that the terabytes of useful data that will soon be released on government websites will come at a cost to privacy commensurate with, if not disproportionate to,³⁰⁶ the increase in sunlight and utility.

Quantity

Most privacy laws regulate data quality but not quantity.³⁰⁷ Laws dictate what data administrators can do with data according to the nature, sensitivity, and linkability of the information, but they tend to say nothing about how much data a data administrator may collect, nor how long the administrator can retain it. Yet, in every reidentification study cited, the researchers were aided by the size of the database. Would-be reidentifiers will find it easier to

300. Data.gov, About <http://www.data.gov/about> (last visited June 12, 2010) ("The purpose of Data.gov is to increase public access to high value, machine-readable datasets generated by the Executive Branch of the Federal Government").

301. See Posting of Nate Anders on, *Obama Appoints Virginia's Aneesh Chopra US CTO*, ARSTECHNICA LAW & DISORDER BLOG, <http://arstechnica.com/tech-policy/news/2009/04/obama-appoints-virginias-aneesh-chopra-us-cto-irs> (Apr. 20, 2009, 13:01 EST).

302. See Posting of Brian Knowlton, *White House Names First Chief Information Officer*, N.Y. TIMES CAUCUS BLOG, <http://thecaucus.blogs.nytimes.com/2009/03/05/white-house-names-first-chief-information-officer> (Mar. 5, 2009, 10:06 EST).

303. *Id.* ("Mr. Kundra discussed some of his plans and interests, including his intention . . . to create a data.gov web site that will put vast amounts of government information into the public domain.")

304. E.g., Posting of Clay Johnson, *Redesigning the Government: Data.gov*, SUNLIGHTLABS.COM, <http://www.sunlightlabs.com/blog/2009/04/16/redesigning-government-datagov> (Apr. 16, 2009, 11:52 EST); Posting by Infosthetics, *Data.gov: How to Open Up Government Data*, INFORMATION AESTHETICS BLOG, http://infosthetics.com/archives/2009/03/open_up_government_data.html (Mar. 13, 2009, 17:25 EST). But see David Robinson, Harlan Fu, William P. Zeller & Edward W. Felten, *Government Data and the Invisible Hand*, 11 YALE J.L. & TECH. 160, 161 (2009) (discussing how the federal government should structure systems to enable greater internet-based transparency).

The Center for Democracy and Technology has posted a supportive but more cautious memo, flagging concerns about Data.gov involving deidentification and reidentification. Ctr. for Democracy & Tech., *Government Information, Data.gov and Privacy Implications*, <http://www.cdt.org/policy/government-information-datagov-and-privacy-implications> (July 13, 2009) ("While Data.gov has great potential, there are important privacy implications associated with data disclosure").

305. See *supra* Part III.B.1.a.

306. See *supra* Part III.B.1.b.

307. See *supra* Part II.A.3 (listing privacy statutes that draw distinctions based on data type).

match data to outside information when they can access many records indicating the personal preferences and behaviors of many people. Thus, lawmakers should consider enacting new quantitative limits on data collection and retention.³⁰⁸ They might consider laws, for example, mandating data destruction after a set period of time, or limiting the total quantity of data that may be possessed at any one time.

Motive

In many contexts, sensitive data is held only by a small number of actors who lack the motive to reidentify.³⁰⁹ For example, rules governing what academic researchers can do with data should reflect the fact that academic researchers rarely desire to reidentify people in their datasets. A law that strictly limits information sharing for the general public—think FERPA (student privacy), HIPAA (health privacy), or ECPA (electronic communications privacy)—might be relaxed to allow researchers to analyze the data with fewer constraints. Of course, regulators should draw conclusions about motive carefully, because it is hard to predict who the adversary is likely to be, much less divine his or her motive.

Regulators should also weigh economic incentives for reidentification. Although we should worry about our enemies targeting us to learn about our medical diagnoses, we should worry even more about financially-motivated identity thieves looking for massive databases that they can use to target thousands simultaneously.³¹⁰

Trust

The flip side of motive is trust. Regulators should try to craft mechanisms for instilling or building upon trust in people or institutions. While we labored

308. See European Union Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Relating to Search Engines*, 00737/EN WP 143 at 19 (Apr. 4, 2008), available at http://ec.europa.eu/justice_home/sj/privacy/docs/wpdocs/2007/wp136_en.pdf [hereinafter 2008 Working Party Opinion] (arguing that search engines should store queries for a maximum of six months).

309. Cf. EU Data Protection Directive, *supra* note 3, at recital 26 (noting that “the means likely reasonably to be used” to identify individuals are relevant to a determination of whether individuals are “identifiable”).

310. As one commentator puts it:
[T]here's far less economic incentive for a criminal to go after medical data instead of credit card information. It's harder to monetize the fact that I know that Judy Smith of Peoria has heart disease—by filing false claims in her name, for example—than to have Judy's credit card number and expiration date. If I'm a criminal with advanced data skills and I have a day to spend, I'm going to go after financial data and not health data.

Cline, *supra* note 177.

under the shared hallucination of anonymization, we trusted the technology, so we did not have to trust the recipients of data; now that we have lost trust in the technology, we need to focus more on trust in people. We might, for example, conclude that we trust academic researchers implicitly, government data miners less, and third-party advertisers not at all, and we can build these conclusions into law and regulation.

2. Applying the Test

By applying the five factors, regulators will have a rough sense of the risk of reidentification of a particular type of provider in a particular context. If the risk is very low, regulators might choose to do nothing. If the risk is very high, regulators should feel inclined to act, imposing new restrictions on data collection, use, processing, or disclosure, and requiring specific data safe-handling procedures.

Regulators should perhaps also take into consideration the sensitivity of the data. It makes sense to treat medical diagnoses differently than television-watching habits, for example, because the path to harm for the former is shorter and more direct than for the latter. But because the database of ruin can be built almost entirely with nonsensitive data, regulators should beware not to make too much of this step in the analysis.

Finally, regulators should compare the risk and the sensitivity to the various benefits of unfettered information flow: for medical privacy, better treatments and saved lives; for internet privacy, better search tools and cheaper products; for financial privacy, fewer identity thefts. If the benefits of unfettered information significantly outweigh the costs to privacy in a particular context, they might decide to surrender.³¹¹ Perhaps lawmakers will see reidentification as the latest example of the futility of attempting to foist privacy on an unappreciative citizenry through ham-handed regulations. Maybe they will conclude they should just give up and live in a society with very little privacy.

Much more often, regulators will conclude that the costs to privacy outweigh the benefits of unfettered information flow. When they come to such a conclusion, they should consider rules and laws that reduce the risk by restricting the amount of information flowing through society. Of course,

311. For example, Harvard's Personal Genome Project, which is sequencing the DNA of thousands of volunteers to hunt for genetic markers for disease, has essentially told its volunteers to forget about privacy. Peter Dizikes, *Your DNA Is a Stretch*, SALON.COM, Feb. 17, 2009, http://www.salon.com/env/feature/2009/02/17/genetic_testing/ ("[T]he Personal Genome Project essentially tell[s] its volunteers to forget about privacy guarantees. 'I like the Personal Genome Project approach,' [one scholar] says. 'It's honest. They're saying, 'If you want to take the risks, great.'")

such restrictions must be chosen with care because of the important values of free information flow. Regulators should thus try to clamp down on information flow in targeted ways, using the factors listed above in their instrumental sense as a menu of potential interventions.

If the costs significantly outweigh the benefits of information flow, regulators might completely ban the dissemination or storage of a particular type of information. For example, regulators should probably often conclude that public releases of information—even information that seems benign or nonthreatening—should be banned, particularly because such information can be used to supply middle links in long chains of inferences. In more balanced situations, regulators might restrict but not cut off information flow, for example by instituting a quantity cap or a time limit for storage.³¹² They might also place even milder restrictions on small classes of trusted people—academic researchers, for example—while banning the sharing of the data with anybody else.

D. Two Case Studies

To demonstrate how a regulator should apply this test, and to highlight the important roles of context and trust, let us revisit again the case studies introduced before: health and internet usage information. Debates about the proper regulation of these two classes of data have raged for many years. Although I cannot capture every nuance of these debates in this space, I revisit them in order to show how to regulate data privacy after the fall of the robust anonymization assumption.

1. Health Information

Once regulators choose to scrap the current HIPAA Privacy Rule—a necessary step given the rule's intrinsic faith in reidentification—how should they protect databases full of sensitive symptoms, diagnoses, and treatments? Consider one class of users of such information in particular: medical researchers seeking new treatments and cures for disease. In this context, both the costs and benefits of unfettered use are enormous. On the one hand, if our worst enemies get hold of our diagnoses and treatments, they can cause us great embarrassment or much worse. On the other hand, researchers use this information to cure disease, ease human suffering, and save lives. Regulators

312. See 2008 Working Party Opinion, *supra* note 308, at 19 (arguing search engines should store queries for only six months).

will justifiably be reluctant to throttle information flow too much in this context since the toll of such choices might be measurable in human lives lost.

HIPAA tried to resolve this dilemma by trusting the technology of anonymization. We no longer trust the technology, but we can still rely on a different trust: trust in the researchers themselves. Health researchers are rarely willing to release sensitive data—scrubbed or not—to just anybody who asks. Instead, they tend to share such data only after verifying the bona fides of the person asking. Regulators should build upon such human networks of trust in a revised HIPAA, allowing data transfer where trust is high and forbidding it where trust is low.

The problem is that today researchers trust one another according to informal rules and soft intuitions, and to build trust into law, these rules and intuitions must be formalized and codified. Should HIPAA rely only on a researcher's certification of trust in another, or should an outside body such as an Institutional Review Board review the bases for trust?³¹³ Should trust in a researcher extend also to her graduate students? To her undergraduate lab assistants? Regulators should work with the medical research community to develop formalized rules for determining and documenting trusted relationships.

Once the rules of verifiable trust are codified, regulators can free up data sharing between trusted parties. To prevent abuse, they should require additional safeguards and accountability mechanisms. For example, they can prescribe new sanctions—possibly even criminal punishment—for those who reidentify. They can also mandate the use of technological mechanisms: both *ex ante* like encryption and password protection, and *ex post* review methods like audit trail mechanisms.

Regulators can vary these additional protections according to the sensitivity of the data. For example, for the most sensitive data such as psychotherapy notes and HIV diagnoses, the new HIPAA can mandate an NSA-inspired system of clearances and classifications; HIPAA can require that researchers come to the sensitive data rather than letting the data go to the researchers, requiring physical presence and in-person analysis at the site where the data is hosted. At the other extreme, for databases that contain very little information about patients, perhaps regulators can relax some or all of the additional protections.

While these new, burdensome requirements on their own might stifle research, they would permit a rather change from the status quo that might instead greatly *expand* research: With the new HIPAA, regulators should

313. According to federal rules, federally-funded research involving human subjects must be approved by an IRB. 45 C.F.R. §§ 46.101–109 (2009).

rescind the current, broken deidentification rules. Researchers who share data according to the new trust-based guidelines will be permitted to share *all* data, even fields of data like birth date or full ZIP code that they cannot access today.³¹⁴ With more data and more specific data, researchers will be able to produce more accurate results, and thereby hopefully come to quicker and better conclusions.³¹⁵

This then should be the new HIPAA. Researchers should be allowed to release full, unscrubbed databases to verifiably trusted third parties, subject to new controls on use and new penalties for abuse. Releases to less-trusted third parties should fall, of course, under different rules. For example, trust should not be transitive. Just because Dr. A gives her data to trusted Dr. B does not mean that Dr. B can give the data to Dr. C, who must instead ask Dr. A for the data. Furthermore, releases to nonresearchers such as the marketing arm of a drug company should fall under very different, much more restrictive rules.

2. IP Addresses and Internet Usage Information

Lastly, consider again the debate in the European Union about data containing IP addresses. Recall that every computer on the internet, subject to some important exceptions, possesses a unique IP address that it reveals to every computer with which it communicates. A fierce debate has raged between European privacy advocates who argue that IP addresses should qualify as "personal data" under the Data Protection Directive³¹⁶ and online companies, notably Google, who argue that in many cases they should not.³¹⁷ European officials have split on the question,³¹⁸ with courts and regulators in Sweden³¹⁹

314. It makes sense to continue to prohibit the transfer of some data, such as names, home addresses, and photographs that could reveal identity without any outside information at all.

315. The current HIPAA Privacy Rule has itself been blamed for a reduction in data sharing among health researchers.

In a survey of epidemiologists reported in the *Journal of the American Medical Association*, two-thirds said the HIPAA Privacy Rule had made research substantially more difficult and added to the costs and uncertainty of their projects. Only one-quarter said the rule had increased privacy and the assurance of confidentiality for patients.

Nancy Ferris, *The Search for John Doe*, GOV'T HEALTH IT, Jan. 26, 2009, <http://www.govhealthit.com/Article.aspx?id=71456>.

316. 2007 Working Party Opinion, *supra* note 28, at 21, Electronic Privacy Information Center, *Search Engine Privacy*, http://epic.org/privacy/search_engine (last visited Apr. 4, 2010).

317. See sources cited *infra* note 324.

318. For a good summary, see Posting of Joseph Carter, *Was That Your Computer Talking to Me? The EU and IP Addresses as "Personal Data"*, PERKINS COIE DIGESTIBLE LAW BLOG, <http://www.perkinscoie.com/ediscovery/blog/2.aspx?entry=5147> (June 24, 2008, 23:30 EST).

and Spain³¹⁹ deciding that IP addresses fall within the Directive and those in France,³²⁰ Germany,³²¹ and the UK³²² finding they do not.

a. Are IP Addresses Personal?

The debate over IP addresses has transcended EU law, as Google has framed its arguments not only in terms of legal compliance but as the best way to balance privacy against ISP need.³²³ In this debate, Google has advanced arguments that rely on the now discredited binary idea that typifies the PII mindset: Data can either be identifiable or not. Google argues that data should be considered personal only if it can be tied by the data administrator to one single human being. If instead the data administrator can narrow an IP address down only to a few hundred or even just a few human beings—in other words, even if the administrator can reduce the entropy of the data significantly—Google argues that it should not be regulated. By embracing this idea, Google has downplayed the importance of information entropy, the idea that we can measure and react to imminent privacy violations before they mature.

Google frames this argument in several ways. First, it argues that IP addresses are not personal because they identify machines, not people.³²⁵ Google's Global Privacy Officer Peter Fleischer, offers hypothetical situations

319. John Oates, Sweden, *IP Addresses are Personal Unless You're a Pirate*, REGISTER, June 18, 2009, available at http://www.theregister.co.uk/2009/06/18/sweden_ip_law.

320. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, STATEMENT ON SEARCH ENGINES (2007), available at http://www.sinnuevar.com/ajpdkanal/documentacion/recomendaciones/comunicacion/pdfs/declaracion_aepd_buscadores_en.pdf (opinion of Spanish Data Protection Agency deciding that search engines process "personal data," relying in part on earlier rulings about IP addresses).

321. Meryem Marzouki, *Is the IP Address Still a Personal Data in France?*, EDRI GRAM, Sept. 12, 2007, <http://www.edri.org/cdngram/num1er5.17/ip-personal-data-fr>.

322. Posting of Jeremy Mittma, *German Court Rules That IP Addresses Are Not Personal Data*, PROSKAUER PRIVACY LAW BLOG: <http://privacylaw.proskauer.com/2008/10/articles/european-union/german-court-rules-that-ip-addresses-are-not-personal-data> (Oct. 17, 2008).

323. INFO. COMM'N'S OFFICE, DATA PROTECTION GOOD PRACTICE: COLLECTING PERSONAL INFORMATION USING WEBSITES 3 (2007), available at http://www.icco.gov.uk/uploads/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_3_1.0.pdf.

324. Posting of Alma Whitten, *Are IP Addresses Personal?*, GOOGLE PUBLIC POLICY BLOG, <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html> (Feb. 22, 2008, 12:31 EST) (tying the discussion to the broad question "as the world's information moves online, how should we protect our privacy?"); Peter Fleischer, *Can a Website Identify a User Based on IP Address?*, PETER FLEISCHER, PRIVACY . . . <http://peterfleischer.blogspot.com/2008/02/can-website-identify-user-based-on-ip.html> (Feb. 15, 2008) ("Privacy laws should be about protecting identifiable individuals and their information, not about undermining individualization."). Mr. Fleischer serves as Google's Global Privacy Counsel. Because of this, I cite his blog posts for clues about Google's views, but I should be clear that Mr. Fleischer's blog bears the disclaimer, "these ruminations are mine, not Google's."

325. Cf. Fleischer, *supra* note 324 (An IP address "constitutes by no means an indirectly nominative data of the person in that it only relates to a machine, and not to the individual who is using the computer in order to commit a counterfeit." (quoting decision of the Paris Appeals Court))

in which many users share one computer with a single IP address, such as "the members of an extended family each making use of a home pc, a whole student body utilising a library computer terminal, or potentially thousands of people purchasing from a networked vending machine."³²⁶ Is Fleischer right to categorically dismiss the threat to privacy in these situations? Is there no threat to privacy when Google knows that specific search queries can be narrowed down to the six, seven, maybe eight members of an extended family? For that matter, should regulators ignore the privacy of data that can be narrowed down to the students on a particular college campus, as Fleischer implies they should?

Second, in addition to the machine-not-person argument, Google further ignores the lessons of easy reidentification by assuming it has no access to information that it can use to tie IP addresses to identity. On Google's official policy blog, Software Engineer Alma Whitten, a well-regarded computer scientist, asserts that "IP addresses recorded by every website on the planet *without additional information* should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings."³²⁷ Whitten's argument ignores the fact that the world is awash in rich outside information helpful for tying IP addresses to places and individuals.

For example, websites like Google never store IP addresses devoid of context; instead, they store them connected to identity or behavior. Google probably knows from its log files, for example, that an IP address was used to access a particular email or calendar account, edit a particular word processing document, or send particular search queries to its search engine. By analyzing the connections woven throughout this mass of information, Google can draw some very accurate conclusions about the person linked to any particular IP address.³²⁸

Other parties can often link IP addresses to identity as well. Cable and telephone companies maintain databases that associate IP addresses directly to names, addresses, and credit card numbers.³²⁹ That Google does not store these data associations on its own servers is hardly the point. Otherwise, national

326. Peter Fleischer, *Are IP Addresses "Personal Data"?*, PETER FLEISCHER: PRIVACY..., <http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html> (Feb. 5, 2007, 17:18 EST).

327. Whitten, *supra* note 324 (emphasis added).

328. See 2008 Working Party Opinion, *supra* note 308, at 21 ("The correlation of customer behaviour across different personalised services of a search engine provider . . . can also be accomplished by other means, based on . . . other distinguishing characteristics, such as individual IP addresses.").

329. *Id.* at 11, 16.

IP numbers in the hands of private parties would not be "personal data" because only the government can authoritatively map these numbers to identities.³³⁰

Google can find entropy-reducing information that narrows IP addresses to identity in many other places: Public databases reveal which ISP owns an IP address³³¹ and sometimes even narrow down an address to a geographic region;³³² IT departments often post detailed network diagrams linking IP addresses to individual offices; and geolocation services try to isolate IP addresses to a particular spot on the Earth.³³³ In light of the richness of outside information relating to IP addresses and given the power of reidentification, Google's arguments amount to overstatements and legalistic evasions.

Google's argument that it protects privacy further by deleting a single octet of information from IP addresses is even more disappointingly facile and incorrect. An adversary who is missing only one of an IP address's four octets can narrow the world down to only 256 possible IP addresses.³³⁴ Google deserves no credit whatsoever for deleting partial IP addresses; if there is a risk to storing IP addresses at all, Google has done almost nothing to reduce that risk, and regulators should ask them at the very least to discard all IP addresses associated with search queries, following the practice of their search-engine competitors, Microsoft and Yahoo.³³⁵

b. Should the Data Protection Directive Cover Search Queries?

Not only does the easy reidentification result highlight the flaws in Google's argument that IP addresses are not personal, it also suggests that European courts should rule that the EU Directive covers IP addresses. Recall that the Directive applies broadly to any data in which a "person . . . can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological,

330. Fleischer correctly points out that ISPs are often forbidden from disclosing the user associated with an IP address. Fleischer, *supra* note 324 ("[T]he ISP is prohibited under US law from giving Google that information, and there are similar legal prohibitions under European laws.") This is no different from any other kind of account number which can be authoritatively tied to identity only by the issuing entity. All other entities must make educated guesses.

331. E.g., ARIN WHOIS Database Search, <http://ws.arin.net/whois> (last visited June 12, 2010) ("ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN.").

332. ERIC COLF & RONALD KRUTZ, NETWORK SECURITY BIBLE 316-18 (2005) (discussing reverse DNS queries).

333. E.g., IP2Location.com, <http://www.ip2location.com> (last visited June 12, 2010); Quova, <http://www.quova.com> (last visited June 12, 2010).

334. An octet is so named because it contains eight bits of data. $2^8 = 256$.

335. See *supra* note 300.

mental, economic, cultural or social identity.³³⁶ Because websites can often tie IP addresses to individual people, the Directive should apply to them. Still, courts in Germany, France, and the UK have held to the contrary. Should the EU amend the Directive to even more unequivocally cover IP addresses?

The answer is not to expand the Directive to specifically cover IP addresses, as we might have done when we still organized laws solely around PH. Instead, the EU should enact new, sectoral regulations that reflect a weighing of costs and benefits for specific problems. In this case, rather than ask whether any company holding an IP address should bear the burden of the EU Directive, the EU might ask whether the benefit of allowing search engines in particular to store and disclose information—including IP addresses associated with search queries—outweighs the potential harm to privacy.³³⁷

I must save for another day a complete response to this question, but to demonstrate the new test for deciding when to regulate after the fall of anonymization, I will outline why I think search engines deserve to be regulated closely. Compare the benefits and costs of allowing unfettered transfers of stored search queries to the earlier discussion about health information, taking the benefits first. By analyzing search queries, researchers and companies can improve and protect services, increase access to information, and tailor online experiences better to personal behavior and preferences.³³⁸ These are important benefits, but not nearly as important as improving health and saving human lives.

On the other side of the ledger, the costs to privacy of unfettered access are probably as great for search query information as for health information, if not greater. As the AOL breach revealed, stored search queries often contain user-reported health symptoms.³³⁹ In fact, Google takes advantage of this to track and map influenza outbreaks in the U.S.³⁴⁰ When one considers how often Google users tell Google about symptoms that never escalate to a visit to the doctor, one can see how much richer—and thus more sensitive—this information can be than even hospital data.

We reveal even more than health information to search engines, supplying them with our sensitive thoughts, ideas, and behavior, mixed in of course with

336. EU Data Protection Directive, *supra* note 3, art. 1(a).

337. In the EU, the Article 29 Working Group privacy watchdog has proposed similarly special treatment for search engines. 2008 Working Party Opinion, *supra* note 308, at 24.

338. See *supra* note 201.

339. Barzuo & Zeller, *supra* note 69 ("Her search history includes 'land tremors,' 'nicotine effects on the body,' 'dry mouth' and 'bipolar.' But in an interview, Ms. Arnold said she routinely researched medical conditions for her friends to assuage their anxieties.").

340. Google.org, Flu Trends, <http://www.google.org/flu Trends> (last visited June 12, 2010).

torrents of the mundane and unthreatening.³⁴¹ In an earlier article, I argued that the scrutiny of internet usage—in that case by Internet Service Providers—represents the single greatest threat to privacy in society today.³⁴² Regulators have underappreciated the sensitive nature of this data, but events like the AOL data release have reawakened them to the special quality of stored search queries.³⁴³

Because the costs of unfettered data access are as high in the search-engine as in the health context, EU and U.S. regulators should consider enacting specific laws to govern the storage and transfer of this information. Because the benefits are less than for health information, regulators should be willing to restrict the storage and flow of search query information even more than HIPAA restricts health information.

Thus, the EU and U.S. should enact new internet privacy laws that focus on both the storage and transfer of search queries. They should impose a quantity cap, mandating that companies store search queries for no longer than a prescribed time.³⁴⁴ They should set the specific time limit after considering search companies' claims that they must keep at least a few months' worth of data to serve vital business needs. They should also significantly limit third-party access to search query data.

CONCLUSION

Easy reidentification represents a sea change not only in technology but in our understanding of privacy. It undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations. Regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from unwanted, significant harm. They must do this without leaning on the easy-to-apply, appealingly nondisruptive, but hopelessly flawed crutch of personally identifiable information. This Article offers the difficult but necessary way forward: Regulators must use the factors provided to assess the risks of reidentification and carefully balance these risks against countervailing values.

341. Cf. Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

342. Paul Ohm, *The Rise and Fall of ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1417.

343. See 2008 Working Party Opinion, *supra* note 308, at 8 ("Search engine: play a crucial role as a first point of contact to access information freely on the internet.").

344. Cf. *id.* at 19 ("[T]he Working Party does not see a basis for a retention period beyond 6 months").

250

Although reidentification science poses significant new challenges, it also lifts the veil that for too long has obscured privacy debates. By focusing regulators and other participants in these debates much more sharply on the costs and benefits of unfettered information flow, reidentification will make us answer questions we have too long avoided. We face new challenges, indeed, but we should embrace this opportunity to reexamine old privacy questions under a powerful new light.

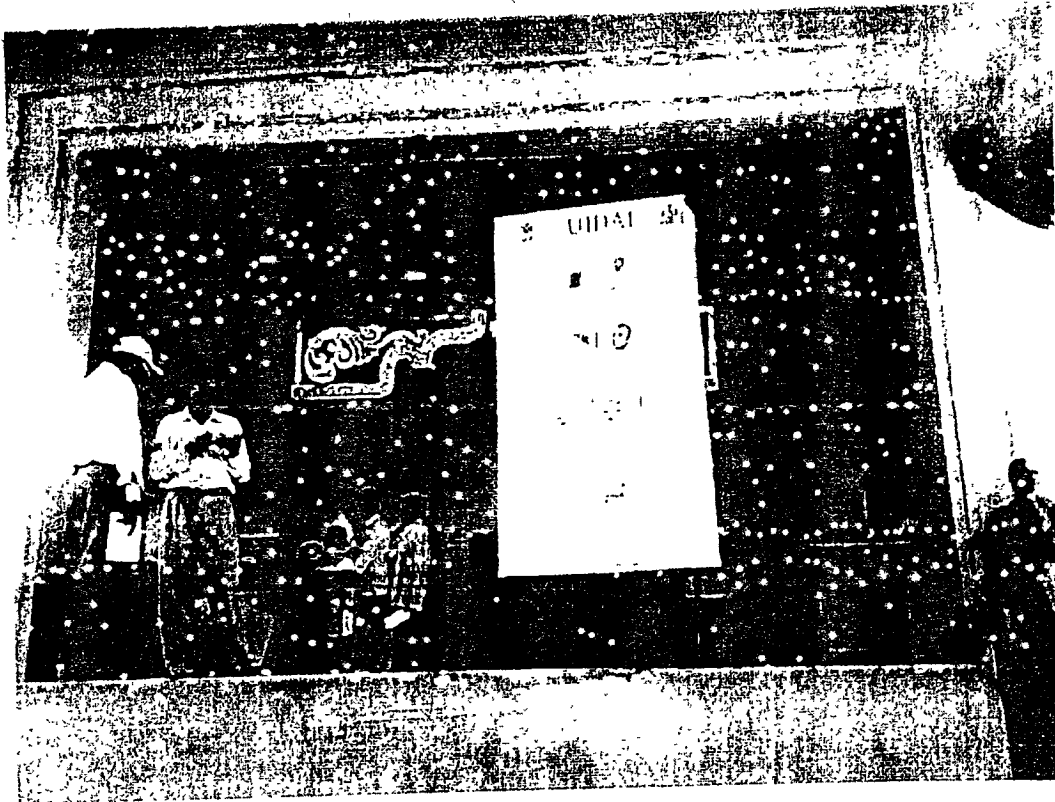
UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

41 - 'I'

PK 6101/12

251



UID Enrolment Proof-of-Concept Report

252

Table of Contents

| | |
|--|------------------------------|
| Introduction | 3 |
| Goals..... | Error! Bookmark not defined. |
| Executive summary of outcome..... | 4 |
| Chronology of planning and execution..... | 5 |
| Choice of locations | 5 |
| Biometric devices | 9 |
| Preparation of enrolment agency and software | 9 |
| Pre-enrolment field and data preparation | 10 |
| Enrolment Process..... | 13 |
| Process Variations | 14 |
| Enrolment software | 16 |
| Reenrolment Rates..... | 17 |
| Observations | 19 |
| Process observations | 20 |
| Biometric observations..... | 22 |
| Conclusion..... | 24 |
| Annexure 1 - Enrolment application screen shots | 25 |
| Annexure 2 – Enrolment times by age and demographics | 29 |
| Enrolment times by age | 29 |
| Enrolment times by occupation | 29 |
| Enrolment times by gender | 29 |
| Annexure 3 – Biometric matching accuracy curves | 30 |

Introduction

The UID Authority of India conducted a Proof-of-Concept (PoC) study of biometric enrolment from March 2010 to June 2010 in the predominantly rural areas of Andhra Pradesh, Karnataka, and Bihar. The UIDAI also carried out the biometric enrolment of school children in the vicinity of Bangalore. About seventy five thousand people in all were enrolled during the first phase of the PoC study, and sixty thousand of the same people were re-enrolled during the second phase after a gap of three weeks.

Prior to conducting the UIDAI PoC, there was insufficient reliable biometric data available for residents of India that could be used to analyze and reach conclusions relevant to the implementation of the UID program. In addition, outside the state of Andhra Pradesh, there was no significant history of collecting iris images. In the last five years, iris image capture devices have gone through significant technological advances. There was however, limited data available from anywhere in the world regarding the ease of iris capture, as well as the usability of iris images in the case of minors. Therefore, the UIDAI felt it necessary to conduct Proof-of-Concept studies for biometric enrolment in several states, and analyze the data.

This report chronicles these Postludes. The report consists of a narrative of the activities, observations and conclusions based on numerous visits to the enrolment sites, and conclusions inferred through i) the statistical analysis of the processes and ii) by biometric analysis of the data collected during the studies.

In the study, face photos, iris images, and fingerprints of all ten fingers were captured. The ten fingerprints were captured in two different ways, first using a slap device, and then using a single finger device. Rural areas were emphasized in the study for two reasons. One was the uneven quality of fingerprints expected from rural workers whose fingerprints could be worn out by prolonged physical labour. The second was to test the UIDAI's ability to carry out biometric enrolment in locations representative of the majority of India's infrastructure, i.e. in areas with limited access to electrical power, proper lighting, and other support systems.

Objectives

The enrolment PoC was conducted to evaluate technical, operational, and behavioural hypotheses related to both the use of biometric devices and the overall enrolment process itself. It was also conducted to establish a baseline for the quality of biometric data that could be collected in rural India.

Technical objectives

- i) Measure the biometric quality that could be achieved in rural Indian conditions
- ii) Understand the difficulty challenges in capturing iris images,

254

iii) Determine suitable ergonomics in the use of the biometric devices, and understand the optimal overall layout of the enrolment station.

Operational objectives

i) Carry out a time and motion study through observation, as well as an analysis of process data collected through the client software.

Behavioural objectives

i) Understand how people in rural India would respond to the capture of iris images. This was an important goal, since data on the experience of the public with iris capture devices is limited, compared to studies on fingerprint capture

ii) Overall response of enrollees to the entire biometric capture process in the PoC needed to be understood

There were also more intangible lessons that would be directly applicable to the actual UID enrolment, since the PoC was designed to mimic UID enrolment. For instance, it was expected that the PoC experience would enable the UID team to tailor biometric enrolment best practices to be more applicable in Indian conditions

Executive summary of outcome

1. The PoC successfully conducted over 135,000 biometric enrolments. The relative ease of conducting the operation confirmed that biometric enrolment conforming to UID standards of quality and process was indeed possible on a large scale in rural India. The total biometric enrolment time for each individual, on average, was a little over three minutes. Of this, iris enrolment took a little under a minute, and was not perceived to be excessively difficult either by the resident or the enrolling operator. Specifically, many blind people had their iris images captured (For details, see table Page 19)
2. Multiple fingerprint scanners as well as iris capture devices were used in the PoC, and they performed according to expectations. The PoC was dispersed geographically and included many rural, often remote locations across three states. The enrolment was typically conducted with minimal infrastructure and sometimes in extreme weather conditions. Enrolees varied in age all the way from four years to about ninety years of age.
3. Older people took longer to enrol than younger people, and enrolees whose employment involved manual work took longer to enrol than the rest of the PoC population. Older people needed more assistance from operators to capture of their

biometrics. However, the range of enrolment times observed was well within expectations and was not seen as making enrolment impractical.

4. The enrolment variations tested in the process led to the conclusion that the best process was one where the enrollee remained stationary during enrolment and the operator did the positioning of the devices
5. The enrolment of children in the school showed that children in the age range of four to fifteen could be biometrically enrolled using the same process as that used for adults and with no additional difficulty. The match analysis also showed that their iris images and fingerprints could be deduplicated as accurately as those of adults.
6. The quality of the biometric capture was sensitive to the setup of the enrolment station and the process itself. Most importantly, the enrolment operator's instructions made a significant difference in the efficiency of the biometric capture.
7. The quality check process built into the enrolment software was very important and provided helpful feedback to the operator in capturing high quality images.
8. The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually. The multi-modal enrolment was adequate to carry out deduplication on a much larger scale, with reasonable expectations of extending it to all residents of India.

Chronology of planning and execution

It was decided that the PoC would be done in three states: Andhra Pradesh, Karnataka, and Bihar. At least 20,000 sets of biometric data had to be collected in each state. To analyze the accuracy of biometric matching, the same set of biometric samples had to be collected again after a suitable time lag of three weeks. In order to ensure that the 20,000 sets of duplicate data could be collected, the initial enrolment target in each state was 25,000. This would allow for a minority of people not showing up for re-enrolment during the second round.

The regional offices of the UIDAI in conjunction with the technology team worked with the state governments to plan the PoC. In Andhra Pradesh and Karnataka, the Food & Civil Supplies department was designated the nodal agency for the PoC study. In Bihar, the PoC was done in conjunction with enrolment for the NREGS e-Shakti project.

Choice of locations

The following factors were considered while choosing locations for the PoC:

- i) The enrollees at the PoC locations had to be representative of the Indian population in biometric quality. This meant that over eighty percent of the PoC locations

256

- were rural, since the majority of India lives in villages. However, the remaining twenty percent of the PoC sites were urban locations close to large cities, in order to have urban areas well represented in the biometric samples collected.
- ii) A further consideration was that the rural locations should be at least fifty kilometres away from the large metropolitan areas, such as Bangalore or Hyderabad. This was done since a sampling of closer locations showed that the working population of the villages close to metropolitan areas typically commuted to urban locations for work, and in general, the population was more representative of urban populations.
 - iii) The goal of the PoC was to collect data representative of India and not necessarily to find difficult-to-use biometrics. Therefore, extremely remote rural areas, often with populations specializing in certain types of work (tea plantation workers, areca nut growers, etc.) were not chosen. This ensured that degradation of biometrics characteristic of such narrow groups was not overrepresented in the sample data collected.
 - iv) For the three PoCs (apart from the school PoC), the goal was to enrol adults. In Karnataka and Bihar, only residents above 18 years were allowed to enrol. In Andhra Pradesh, adults were encouraged to enrol and very few minors actually enrolled.

The state nodal agencies in collaboration with the UID team and the enrolment agencies accordingly selected a set of locations to conduct the PoC. In Andhra Pradesh and Karnataka, two districts each were chosen for the PoC. In each district, five villages were selected for enrolling people. In Bihar, the villages scheduled for PoC enrolment was decided by the e-Shakti schedule.

The PoC was subsequently conducted in ten villages each in Karnataka and Andhra Pradesh, and in over thirty villages in Bihar. The choice of villages across states met our goal of geographic diversity since the PoC locations were widely dispersed.

Within each village, the enrolment location selected was usually the local primary school or other public building (photos below). The enrolment agency brought computers, biometric devices and related equipment. In most areas, one or two power generators were also brought to provide reliable power for lighting and computers. The enrolment was carried out using locally available furniture.

PoC enrolment was also conducted in the Deputy Commissioners' offices in Mysore and Tumkur cities. Finally, PoC enrolment for school children between 4 years and 15 years was conducted in a Bangalore school. In Karnataka, the villages chosen were those with Gram Panchayat offices, i.e., larger villages. In Andhra Pradesh and in Bihar, this was not always so. The following is the list of PoC locations.

| Bihar | | |
|----------------|--|----------|
| Gram Panchayat | Revenue Villages | Block |
| Bind | Bind (ward no 4 -14), Bind (Kusar, Bishunpurand & Nirachak) | Bind |
| Jahana | Jahana, Chatarpur, Rampur, Nirpur, Khalsa, & Nigraian | Bind |
| Jamsari | Barhog, Jamsari, & Dariapur | Bind |
| Katrahi | Katrahi, Jakki, Bakra, Makanpur, & Makanpur (Dhullahpur) | Bind |
| Lodipur | Lodipur, Jaitipur, Gajipur, Ibrahimpur | Bind |
| Onda | Onda | Asthawan |
| Tajuipur | Tajuipur, Mahmudabad, Madanchak, Rasalpur, Nauranga, & Rajopur | Bind |
| Utarthu | Utarthu, Masia, Ahiachak, Muftipur | Bind |

| Andhra Pradesh | | |
|----------------|------------------|-------------------------|
| District | Mandal | Village |
| Medak | Tupran | Ghanpur |
| | Wargal | Wargal |
| | Wargal | Veluru |
| | Chegunta | Narsingi |
| | Patacheru | Ward-11 |
| Krishna | Mylavaram | Velvadam |
| | Kruthivennu | Lakshmi puram |
| | Vijayawada Rural | Nidamanuru |
| | Penamaluru | Poranki |
| | (Urban) | Vijayawada Urban Ward 9 |

| Karnataka | | |
|-----------|-----------|------------------------------|
| District | Taluk | Gram Panchayath or DC Office |
| Tumkur | Tumkur | DC Office Staff |
| | Tumkur | Bellavi |
| | Gubbi | Chelur |
| | Madhugiri | Dodderi |
| | Tiptur | Kibbanahalli |
| | Sira | Bukkapatna |
| Mysore | Mysore | DC Office Staff |
| | Mysore | Varuna |

258

| | | |
|-----------|------------------------|----------------------|
| | HD Kote | Pommaragalli |
| | Nanjangud | Hadinaaru |
| | Hunsur | Gowdagere |
| | KR Nagar | Tippuru |
| Bangalore | School: (children PoC) | Poorna Prajna school |



Figure 1 Typical PoC Enrolment location

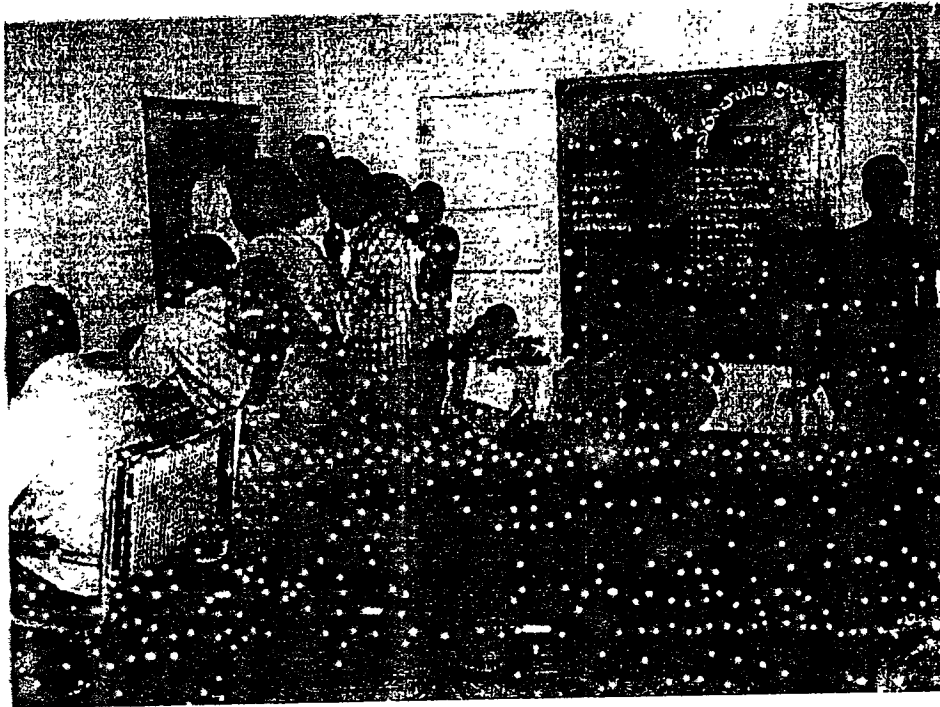


Figure 2 Typical PoC Enrolment room

Biometric devices

Fingerprint scanners and iris capture devices from three different vendors were used in the three PoC states. In Karnataka, the iris devices were from Iris ID (formerly LG Iris) and the fingerprint devices were from Morpho (formerly Sagem). In Bihar, the fingerprint scanner and the iris capture device were both from Crossmatch Technologies. In Andhra Pradesh, the fingerprint scanner and iris capture devices were both from L-1 Identity solutions. In Andhra Pradesh, both a single-eye iris capture device and a two-eye iris capture device were used. The Crossmatch iris devices were binocular type, the L-1 iris devices were hand-held, and the Iris ID iris devices were mounted on tripods, but could also be used as hand-held devices. Using multiple devices added further to the diversity of the PoC process and later enabled us to match images captured using different devices.

Preparation of enrolment agency and software

Enrolment agencies who had already worked with the respective states on previous projects were chosen to implement the PoC by the respective state government agencies. The agencies were 4G ID solutions in Andhra Pradesh, Comat Technologies in Karnataka, and SmarTech Technologies (an arm of Glodyne) in Bihar. In parallel, biometric devices were procured for the PoC. The biometric devices procured were the following: iris capture devices, iris and face capture devices, slap fingerprint scanners, and single finger capture devices.

The enrolment agencies had varying levels of biometric enrolment experience. The UiD technology group worked with each agency to ensure adequate training and prescribed the process flow to be followed.

260

A reference implementation of the enrolment software was created to standardize the process and have a uniform look-and-feel of the application across all three states. However, since the devices used were different in each state, the enrolment software used in each state was a custom version which followed the reference design. The UID technology team worked with each of the three agencies to create the customized software to be used in the corresponding state. There were also variations in the capture process followed, particularly in iris capture, because of the variations in capture devices.

A special feature of the enrolment software was that all biometric images went through a software quality check process. The quality check would indicate a pass or fail based on minimal acceptable quality of the image. If the quality check failed, the image would still be stored, but the operator would be required to recapture the image. The enrolment software entailed the operator to repeat the capture up to four times. The software ensured that the operator was not able to proceed to the next step until the recapture was done.

One important aspect of the enrolment software was the capture of process data along with biometric and demographic data. Thus the number of capture attempts and timestamps captured at numerous points in the capture process were written into an XML file during enrolment. This enabled us to eventually carry out a detailed analysis of the process.

Pre-enrolment field and data preparation

The initial step was to work with the local authorities to find possible enrolment locations and make preparations for getting people to show up. The local authorities typically went house-to-house to inform residents about the date and time they were to enrol. The authorities would also be present at the enrolment centre to ensure that people did show up, resolve any disputes among the enrollees and maintain order. The part played by the local authorities was consequently crucial to the success of the enrolment drive.

The enrolment agency supervisors visited the locations to identify the most suitable building for the enrolment centre, ahead of the start of the PoC. They also arranged for the right furniture among what was available in the building and set up the enrolment stations to meet the PoC needs. One important point was that the table should not be too wide and the heights of the operator, and size of the chairs for the enrollee should accommodate the biometric capture process.

Additionally, it was ensured that there was adequate space for people to wait outside since people crowding around the biometric stations would disturb the process. However, a few chairs were kept nearby for observers since it was felt that each resident observing the process before his or her enrolment would improve the person's ease of enrolment. Posters describing the biometric process (shown in photograph below) were also put up at the door of the enrolment centre to help enrollees familiarize themselves with the process.

In parallel, the demographic data of the residents of the local taluk or mandal was obtained from the food and civil supplies department and loaded into the appropriate laptops. Blank

forms were also kept at the enrolling centres to accommodate people who did not appear in the database, but wished to enrol.

Provisions were made for a bucket of water and towels for residents involved in manual work to clean their hands before enrolment. Also wet and dry clothes were kept at each enrolment station for assisting people with overly dry fingers.

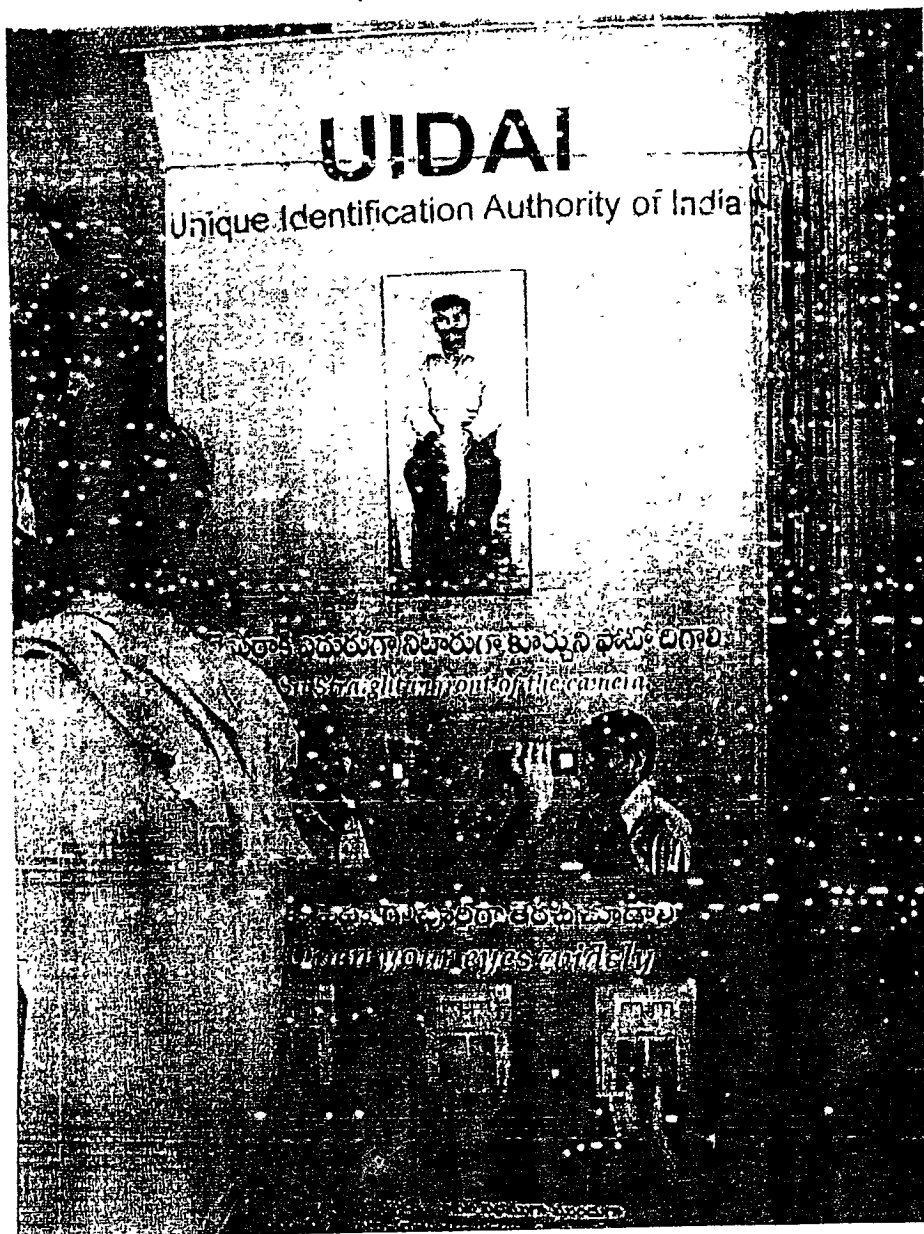


Figure 3 Poster describing biometric capture for residents to observe

262

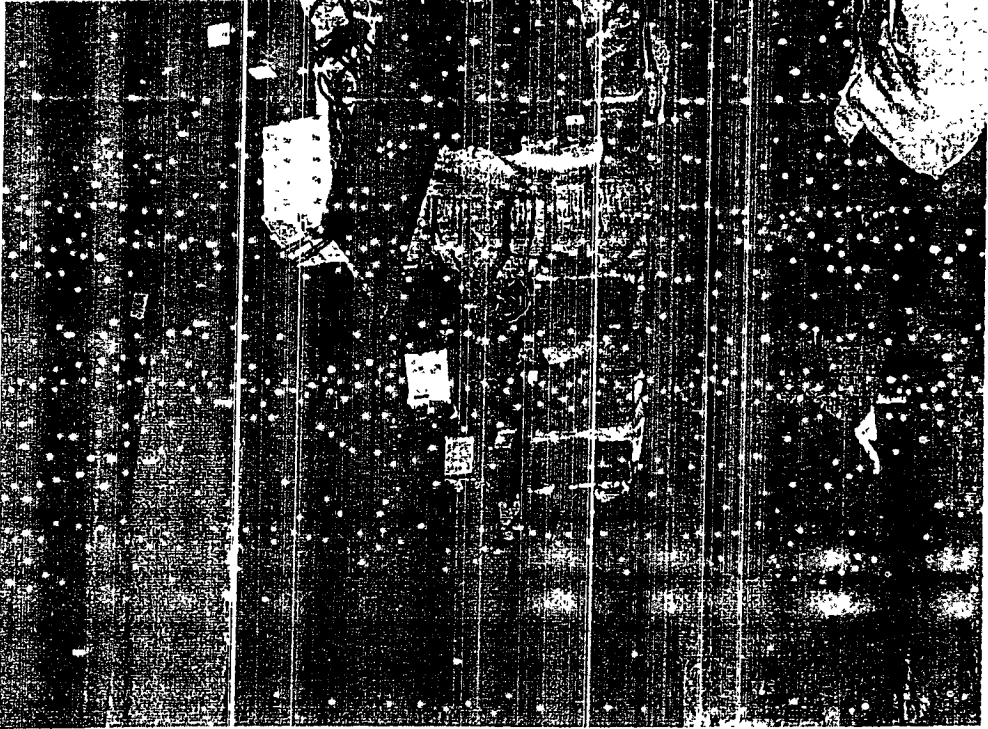


Figure 4 Enrolment stations

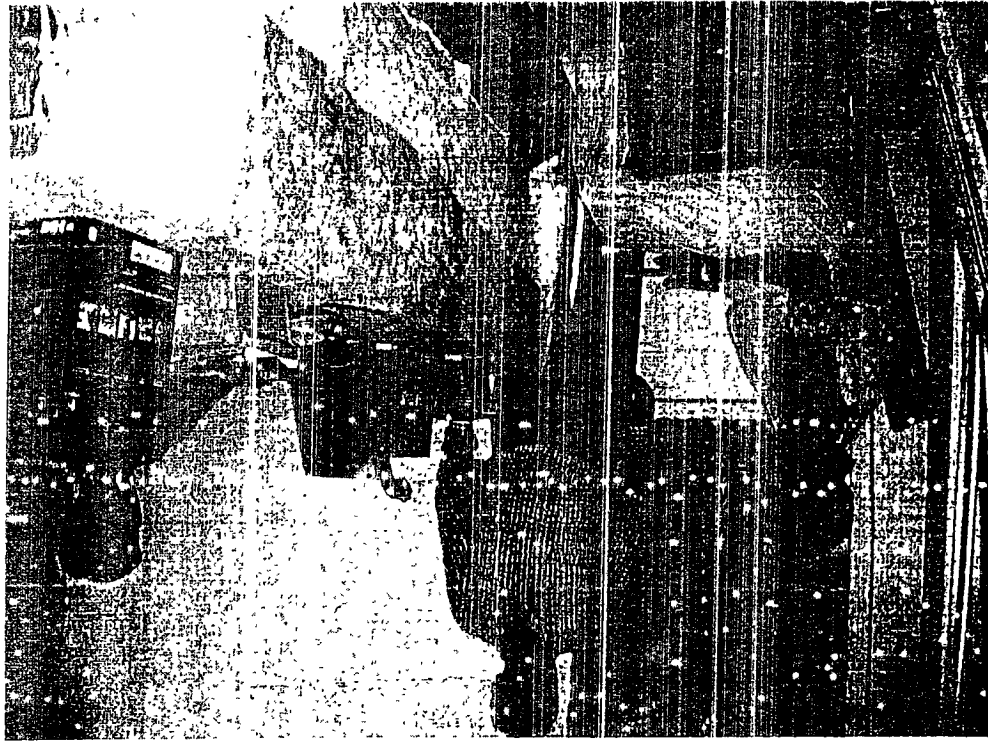


Figure 5 Enrolment station

Enrolment Process

The basic process and associated workflow enforced by the enrolment software is described below. There were minor variations in each state due to the different devices used and the differences in demographic data collection; these variations are listed subsequently.

1. The enrollee would arrive at the enrolling centre with an identifying card. The first station was a non-biometric station where the demographic information of the enrollee was either collected from the card or retrieved from an existing database. A form populated with the demographic information was then printed (or in some cases, forms were printed ahead of time) and any necessary corrections made. The demographic information collected was name, address, date of birth (or age), and occupation.
During the second round of enrolment, the tear-off receipt (described in step 6) was used to identify the application number of the applicant.
Following this the enrollee was sent to an available biometric enrolment station.
2. Using the application number from the application form or first round receipt, the enrollee's demographic record was populated in the enrolment screen. At this point, the operator would check for biometric exceptions (missing fingers or eyes) by asking the enrollee to show his/her hands. If there was an exception, it would be marked in the exception section of the screen, and the information would be stored in the XML file along with the demographic information.
3. Once the above process was completed, the biometric capture would start. The enrollee would first sit down facing the operator and the face photo would be captured by a webcam. The enrolment software would then perform a quality check and crop the image. If the quality check or image cropping failed, the photo would be recaptured up to a maximum of four total attempts. The cropped face photo would be shown on a small frame on the right and it would remain on display during the rest of the biometric capture (see Annexure 1 for screen shots).

A white non-reflecting background screen was placed behind the enrollee's chair to provide a uniform background for face photo capture, and ensure that the background portion of the photo quality check was met. While capturing face photo, the enrollee was instructed to look straight and keep his or her mouth closed.

During the second round of enrolment, the face photo from the first round of enrolment would appear on the application screen so that the operator could confirm that the same person whose biometrics had been captured in the first round was being re-enrolled. After confirming that the photo matched the enrollee, the operator would capture a new face photo which would be cropped, and replace the earlier photo on the screen. The photo would be stored along with the other biometrics in the second round database.

264

4. The iris images of the enrollee were captured with a single-eye or two-eye iris capture device. Based on the results of the quality check, the image(s) would be recaptured for a maximum of four total attempts. While capturing iris image, the enrollee was instructed to look straight into the LEDs, rectangle or other appropriate point (depending on the device), open his or her eyes wide ("look angry or glare") and to not blink.
5. The three slap fingerprint images (4-4-2), i.e. left hand slap, right hand slap, and slap image of the two thumbs, were captured. As above, based on the results of the quality check, the capture would be attempted up to four times. The slap fingerprint capture was done with the enrollee standing. This was to ensure that the person could apply sufficient pressure to be able to get good fingerprints. While capturing fingerprint images, the enrollee was instructed to open their hands, place their fingers flat on the platen in the correct position and press their fingers down firmly.
6. Individual fingerprints of all ten fingers were captured using a single-finger capture device. The individual prints were matched with the corresponding prints from the segmented images of the slap fingerprint captured in step 4. If the fingerprints did not match, step 5 was repeated, while still not exceeding a total of four slap attempts for each type of slap capture. This capture was also done with the enrollee standing.
7. If one or more of the enrollee's fingers or eyes were missing, an exception photograph of the enrollee's face along with both hands opened to show the missing fingers would be captured. This was in order to have a visual record of the missing biometrics.
8. In the first round of enrolment, a tear-off receipt that was printed at the bottom of the application form was given to the enrollee, and the enrollee was asked to bring the tear-off receipt when returning for re-enrolment in the second round.

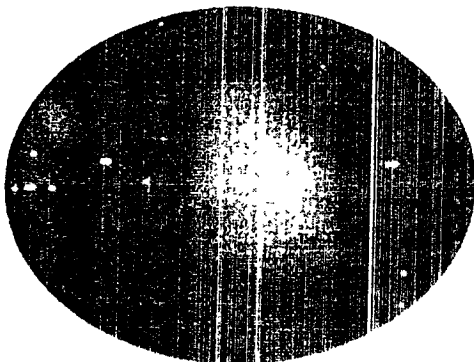


Figure 6 Damaged finger example

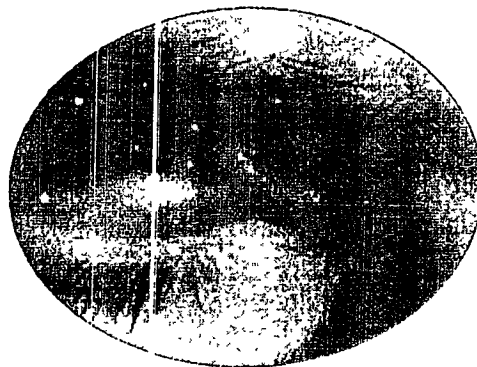


Figure 7 Damaged eye example

Process Variations

1. Identifying document of enrollee: The enrollee would come to the enrolling centre with his or her ration card in the case of Karnataka and Andhra Pradesh. In Bihar, the enrollee was asked to bring his or her job card. Neither of these cards would completely identify the individual since a single ration card listed all members of the family and each job card would list all adult members of the family. So, an additional digit was appended to the ration card or job card number to create an application number identifying the individual.

Collection of demographic information: In Karnataka, a pre-printed form which had the relevant data for the enrollee was chosen from a stack containing forms for all residents of the village sorted by ration card number. This was handed to the enrollee. In Andhra Pradesh, a form containing the enrollee information was printed at the enrolment site and handed over to the enrollee. In Bihar, the enrollees were asked to fill in the form (if necessary, the enrolment agency employee filled the form for the enrollee) and the data was then entered into the application.

2. For iris capture, there were three variations in the three states.
In Bihar, a binocular type iris capture device was used. Ideally, the enrollees would be able to hold the iris device to their eyes unassisted, and wait for the iris capture to complete. In practice, the operator sometimes helped hold the device up, particularly in the case of older enrollees.

In Andhra Pradesh, the operator held the device. The enrollee would stand up and the operator would bring the capture device close to the enrollee's face and then move the device back slowly to capture the iris image. Both single eye devices and dual eye devices were used. Dual eye device were used for about 61.5 percent of the enrolments and the remaining were done using the single eye device.

In Karnataka, a dual eye device was used and it was mounted on a tripod for a large part of the PoC. The resident would move his or her face slowly towards the device and the device would capture the iris image at the appropriate distance. A small portion of the PoC was done using the iris capture device as a hand-held device, where the operator moved the device towards the enrollee's eyes. The PoC done later in the school in Karnataka also used the same dual eye device as a hand held device.

266

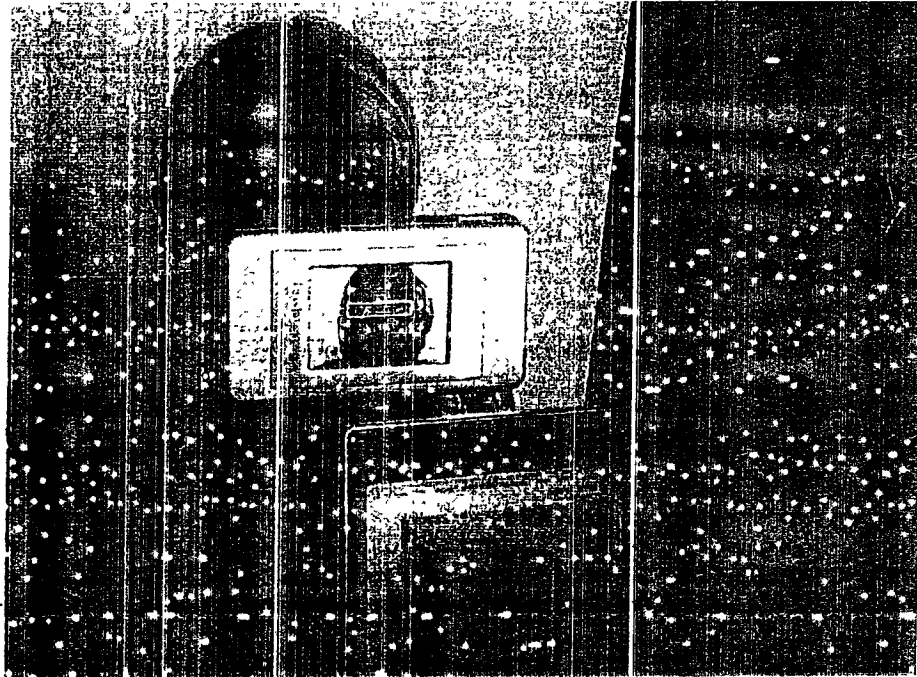


Figure 8: Karnataka- iris camera mounted on a tripod

Enrolment software

The enrolment software had the following screens (Annexure 1)

1. Demographic data and biometric exception capture
2. Face photo capture
3. Dual iris capture
4. Slap fingerprint capture – three slaps to capture all ten fingerprints
5. Capture of ten fingerprints using a single finger device
6. Capture of an exception photograph if necessary

The following are a few noteworthy points related to the enrolment software:

Once the face photo was captured and cropped, it was displayed on a small frame during the capture of all the other biometrics. This would allow the operator to avoid mistakes and avoid combining the biometrics of two different individuals in one enrolment if there was an interruption halfway through the enrolment process.

There were visual biometric quality indicators associated with each image, which the operator could use to quickly gauge image quality (Annexure 1). This was done to avoid the necessity for the operator to interpret quantitative scores.

266
267

The enrolment software would save time stamps during each screen transition, i.e. when moving from one of the screens (1 to 5) listed above to any of the other screens. This was used to measure the "process" time associated with the capture of each biometric. The time measured was not directly related to the time spent by the device to capture the image.

In the context of the UID, the time required for enrolment of each person was a very important factor since it directly translated into the resources needed. Therefore, it was important to record the overall "process" time related to the capture of each biometric and not only the device capture time. For instance, the time measured included the time spent by the operator giving instructions related to the biometric capture, the time spent in the enrollee positioning himself or herself for the specific biometric etc.

Thus the measured times may not be applicable in a different context. In particular, when the enrollee is experienced in the process and if self-enrolment is done, the conclusions reached here would not be valid. Also, the measurement was not designed to measure device efficiency beyond the UID context.

The "process" timestamps and the number of attempts captured by the software allowed us to compute average capture times and the average number of capture attempts per biometric. In conjunction with the age and occupation captured in the demographic screen, we were also able to analyse the average capture time and average number of capture attempts by age and by occupation. This was important since there are several occupations where repeated rubbing and scratching of fingers result in worn out fingerprints.

Finally the software also indicated the number of fingers and eyes for which images could not be captured in each enrolment, because the corresponding finger or eye was missing or damaged. Even in these cases, the remaining biometrics were captured and the enrolment was completed successfully.

Re-enrolment Rates

One of the important goals of the PoC was to create known duplicates by having each enrollee come back after three weeks to be re-enrolled. During the planning of the PoC, there was apprehension that a significant number of enrollees would not come back for re-enrolment. This was a source of concern particularly in Karnataka and Andhra Pradesh, where the PoC was not associated with any ongoing government benefits program and was a standalone experiment. Therefore, incentives were provided for enrollees to re-enrol. In Andhra Pradesh, and Bihar, each enrollee was given seventy rupees following re-enrolment. In Karnataka, a small snack was provided both during the first round and during the second round of enrolment. Despite these efforts, the conservative target rate of re-enrolment was set at eighty percent. Therefore twenty-five thousand people in each state were targeted in the first round to generate matched pair of twenty thousand after the second round. Actual re-enrolment rates were very good and the enrolment agencies were able to reach the targets without much difficulty.

The following are the actual re-enrolment rates observed

Karnataka Re-enrolment Rates

| | Taluk | Gram Panchayath | Enrolment numbers | Reenrolment numbers | Percentage reenrol ling |
|--------|-----------|-----------------|-------------------|---------------------|-------------------------|
| Tumkur | Tumkur | Bellavi | 1,975 | 1,692 | 86 % |
| Tumkur | Gebi | Chelur | 2,262 | 1,747 | 77 % |
| Tumkur | Madhugiri | Doddery | 2,193 | 1,797 | 82 % |
| Tumkur | Tiptur | Kibbanahalli | 2,548 | 2,171 | 85 % |
| Tumkur | Sira | Bukkapatna | 2,257 | 1,615 | 71 % |
| Mysore | Mysore | Varna | 2,283 | 2,097 | 92 % |
| Mysore | HD Kote | Honnaragalli | 2,698 | 2,510 | 93 % |
| Mysore | Nanjangud | Hadinaaru | 1,908 | 1,659 | 87 % |
| Mysore | Hursur | Gowdagere | 2,728 | 2,454 | 90 % |
| Mysore | KR Nagar | Tippuru | 2,754 | 2,331 | 85 % |
| | | Karnataka Total | 23,859 | 20,073 | 84 % |

Andhra Pradesh Re-enrolment Rates

| District | Mandal | Village | Enrolment numbers | Reenrolment numbers | Percentage re-enroling |
|----------|------------------|---------------|-------------------|---------------------|------------------------|
| Medak | Tupran | Ganapur | 2000 | 1819 | 91 % |
| | Wargal | Wargal | 2435 | 2123 | 87 % |
| | Wargal | Veluru | 2095 | 1978 | 94 % |
| | Chegunta | Narsingi | 2756 | 2539 | 92 % |
| | Patancheru | Ward-11 | 2602 | 1187 | 46 % |
| Krishna | Mylavaram | Velvadam | 2826 | 2477 | 88 % |
| | Kruthiveedu | Lakshmi puram | 2481 | 2169 | 87 % |
| | Vijayawada Rural | Nidamanuru | 3031 | 2659 | 88 % |
| | Penamaluru | Poranki | 3114 | 2532 | 81 % |
| | Vijayawada Urban | Ward 9 | 2377 | 1200 | 50 % |
| | | AP Total | 25717 | 20683 | 80 % |

Observations

The following are the observed average capture times and number of attempts

| | | Face photo | Iris | Slap Fingerprints (three images) |
|--------------------------|---|------------|------------|-------------------------------------|
| Adults | Capture times (for all attempts combined) | 34 seconds | 52 seconds | 1 minute 51 seconds |
| Adults | Number of attempts | 1.5 | 1.9 | 1.5 |
| Children (4 to 15 years) | Capture times (for all attempts combined) | 33 seconds | 35 seconds | 1 minute 13 seconds |
| Children (4 to 15 years) | Number of attempts | 1.4 | 3.1 | 1.4 |

The important process time averages are as shown below

Average biometric enrolment time for adults is 3 minutes 17 seconds

Average biometric enrolment time for children (4 to 15 years) is 2 minutes 21 seconds

Capture times analyzed by age, occupation, and gender are listed in Annexure 2

| | Percentage of enrollees |
|---|-------------------------|
| One or more fingers missing or otherwise not capturable | 1.2 % |
| Either or both eyes missing or otherwise not capturable | 0.5 % |
| Missing all 10 finger and both eyes | 0.01 % |

Table: Biometric Exceptions (missing eyes and fingers)

The average time required for capture of face photo, fingerprints of ten fingers and iris image of adults was three minutes and seventeen seconds. Of this, a little over half the time was spent on fingerprint capture. The time for iris capture was a little below one minute, and face photo capture took over half a minute. The iris image capture time varied significantly by age, with people above eighty taking twice as long as people in their twenties. The variation in capture time of fingerprints was lower with the older group taking twenty percent longer than the younger group. One apparent anomaly in fingerprint capture times is that 20 to 30 year old people took longer to have their fingerprint captured than older people. This can possibly be attributed to the fact that they may be engaged in occupations involving heavier physical labour and correspondingly more wear on their fingerprints than their older

270
269-
counterparts. The average capture time for iris images and fingerprints for children were no worse than that for adults. This included the youngest children who were only four years old.

The enrolment time also showed significant variation by occupation, with the occupations involving physical labour showing longer enrolment times. For example, agricultural labourers took about one-third longer to have their fingerprints captured compared with public and private sector employees and other white collar workers. Similarly, for iris capture, the variation was over thirty percent.

There were many blind people who had their iris captured successfully. This was because even though they were blind, their iris was intact. Similarly, many people with worn fingerprints had their fingerprints successfully captured. The table above shows that the percentage of residents enrolled with one or more missing fingers was only a little over one percent and the percentage of enrollees with one or both eyes missing was less than one percent of the total enrollee population.

The enrolment PoC for children showed that the process of enrolling children in the age range of four to fifteen was not significantly harder than that of enrolling adults.

Process observations

An important conclusion reached was that the best possible way for conducting biometric enrolment was to have the enrollee be stationary and have the operator do the positioning of the device.

It was also clear that the operator instructions to the resident were very important. The best results obtained in terms of quality and efficiency was when the operator spent a few seconds *ahead of* each biometric capture clearly explaining what was required on the part of the enrollee, for example "keep eyes wide open", "keep fingers flat on the platen and press hard", etc. This was much more effective than trying to correct the enrollee's gaze, positioning etc *during* the capture of the biometric.

The use of quality check software clearly helped in two ways. The first was that there was a clear message that quality of data collected mattered to the UIDAI and that the quality was going to be monitored. The second was that the operator began to recognize good quality images and over time was well versed in collecting high quality images.

The physical layout of the devices and the ability of the operator to reach out and help the enrollee as required were also seen to be important. Therefore the width of the table had to be small enough so that the operator could reach across. The other option was that the enrollee stood next to the operator on the right side for fingerprint capture.

The ambient light was not always sufficient to capture good quality face photographs even during the day. Table lamps or other artificial lighting was often needed.

The mobile USB tethered iris devices used were adequate for capturing good quality images. In addition, fingerprint images from different devices were matched and there were no

270
271

compatibility issues in doing the matching. In general, the devices worked as expected. The differences in process were much more significant compared to the differences in devices.

Iris enrolment was eminently possible from the operator's perspective and was also well accepted by the enrollee. In fact, the iris capture took less time than fingerprint capture.

Older people sometimes needed assistance in positioning themselves (see picture below) and often required assistance in pressing their fingers hard enough on the platen to get good fingerprints. Children were able to position themselves correctly and maintain the position long enough for successful capture of all three biometrics.

The PoC was conducted in the summer months of April, May and June in Medak district of Andhra Pradesh and in Nalanda district in Bihar. During a few days when the PoC was in progress, the temperature reached 44 degrees Celsius in Nalanda district. Despite the extreme temperature and the fact that no fans were available, enrolment went on normally.

In conclusion, it is clear that it is possible to collect good quality biometrics in rural India despite existing shortages in infrastructure, and the biometric variations within the rural population. Reasonable processes can be specified to undertake enrolment on a much larger scale.

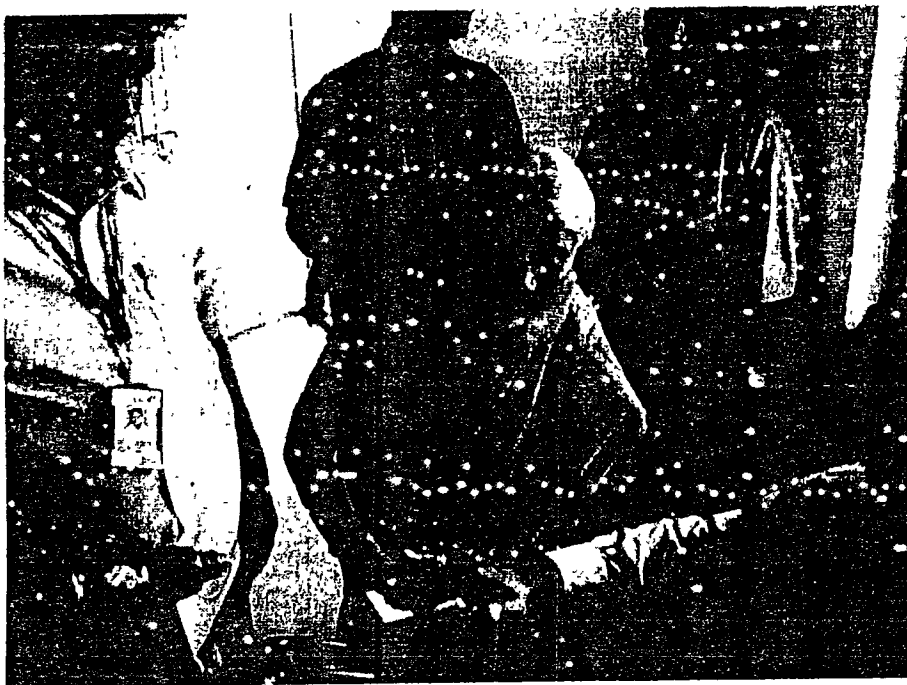


Figure 9: Older resident being assisted with slap fingerprint capture



Figure 10: Eighty six year old resident being assisted with iris capture

Biometric observations

The ultimate goals of biometric enrolment for the UIDAI are two-fold. One is to carry out biometric deduplication for all enrollees in India, and the second is to authenticate the biometrics of an enrolled resident on demand. Therefore, these activities have been the focus of the analysis conducted on the PoC data

Biometric matchability analysis was done on the PoC data to understand the quality of the data and how well it could be used for deduplication and authentication. The basic tool used to study the results is the ROC (Receiver Operational Curve) which shows how two types of potential errors can be traded off against each other for the given set of data. Two of the ROC curves that were obtained from the analysis are shown in Annexure 3 to show a sample of the analysis and to explain the results. The analysis was done using images of ten fingerprints and two irises. The face biometric was not used for matching.

Terminology

The following terminology is needed to understand the results.

Identification: This is the process where any one person's biometrics is matched with that of *all* the other people in the database. This results in establishing the enrollee's biometrics as either unique or as a likely duplicate of the biometrics of an enrollee who had enrolled earlier.

272
273

FPIR: False Positive Identification Rate: This is the likelihood that a person's biometrics is seen as a duplicate (i.e., the biometric deduplication software identifies his biometrics as matching with that of a different person), even though it is not a duplicate in reality.

FNIR: False Negative Identification Rate: This is the likelihood that a person enrolls a second time and the deduplication software is unable to identify their biometrics as a duplicate set.

Verification: This is the process where a person's biometrics is compared only with a copy of his or her biometrics that was captured earlier.

FAR: False Accept Rate: This is the likelihood that a person's biometrics is matched against a different person and the biometrics is seen to match, i.e. the person is wrongly seen to be a different person.

FRR: False Reject Rate: This is the likelihood that a person's biometrics does not match against an earlier sample of his or her biometrics and so he or she is not recognized as the same person.

Results

The matching analysis was done on two sets of 20,000 biometrics, for a total of 40,000. However, the number of comparisons was several orders of magnitude more than 40,000, since each set of fingerprints would be matched against every other set of fingerprints in the data set. Similarly, the iris images from each person would be matched against that of every other person in the data set. Therefore, the results are statistically significant and can be extended to larger populations.

We will now compile the data on the accuracy obtained by enrolling with only fingerprints, enrolling with only iris images, and by enrolling with both biometrics. We will do so using the Identification ROC curve shown in Appendix 3. To compare the accuracies in these three cases, we will look at the point where the FPIR (i.e. the possibility that a person is mistaken to be a different person) is 0.0025 %.

Comparing the FNIR numbers achieved, the FNIR using two irises only is 0.5%, that achieved by using ten fingers only is 0.25%, and that achieved by using ten fingers and two irises is 0.01%. The conclusion we can draw is that accuracy achievable using ten fingerprints is twice that of the accuracy achieved using iris images. Even more important, the accuracy achieved by using ten fingerprints and two irises is fifty times better than by using irises alone and twenty five times better than by using fingerprints alone. The accuracy level achieved was 99.99% in this case.

Looking at the verification ROC for children and adults, we can see that the accuracy obtained in matching for children using iris is better than that for adults. Similarly, the accuracy obtained using fingerprints is better for children than for adults..

By doing analysis as shown in the examples above on real data captured under typical Indian conditions in rural India, we can be confident that biometric matching can be used on a wider

2-711

~~2-73~~

scale to realize the goal of creating unique identities. We have further confirmed that is true as much for children as for adults.

Conclusion

The PoC study was a useful precursor to large scale UID enrolment and has validated our hypotheses regarding biometric enrolment. Iris enrolment was not particularly difficult, and dramatically improved the accuracy levels that could be achieved. The biometric accuracy levels necessary for deduplication of all residents of India are achievable. The time needed for capture of biometrics in typical rural conditions is small enough to support large scale enrolment. In conclusion, the PoC study was a productive part of the ongoing rollout of the UID program.

Annexure 1 - Enrolment application screen shots

274

275

Demographic screen with exception indicators

UID PoC Enrollment Reference Implementation Ver 1.1 RC03

Fields Marked as * are mandatory

English

Application Number: Enrollment ID: Local Language:

Name:

DB Type: ☐ Verified ☐ Declared ☐ Approximate *

Date of Birth: / /

Gender: ☐ Male ☐ Female ☐ TG *

Building:

Street:

Landmark:

Locality:

Village:

Taluka:

District:

State:

Country:

PIN:

Occupation:

Others:

Guardian Name:

Relationship: ☐ Father ☐ Mother ☐ Guardian ☐ Not Given

Guardian Unique ID:

Verification: ☐ Document ☐ Community ☐ Introducer

Introducer Name:

Introducer Unique ID:

Mobile No:

Email:

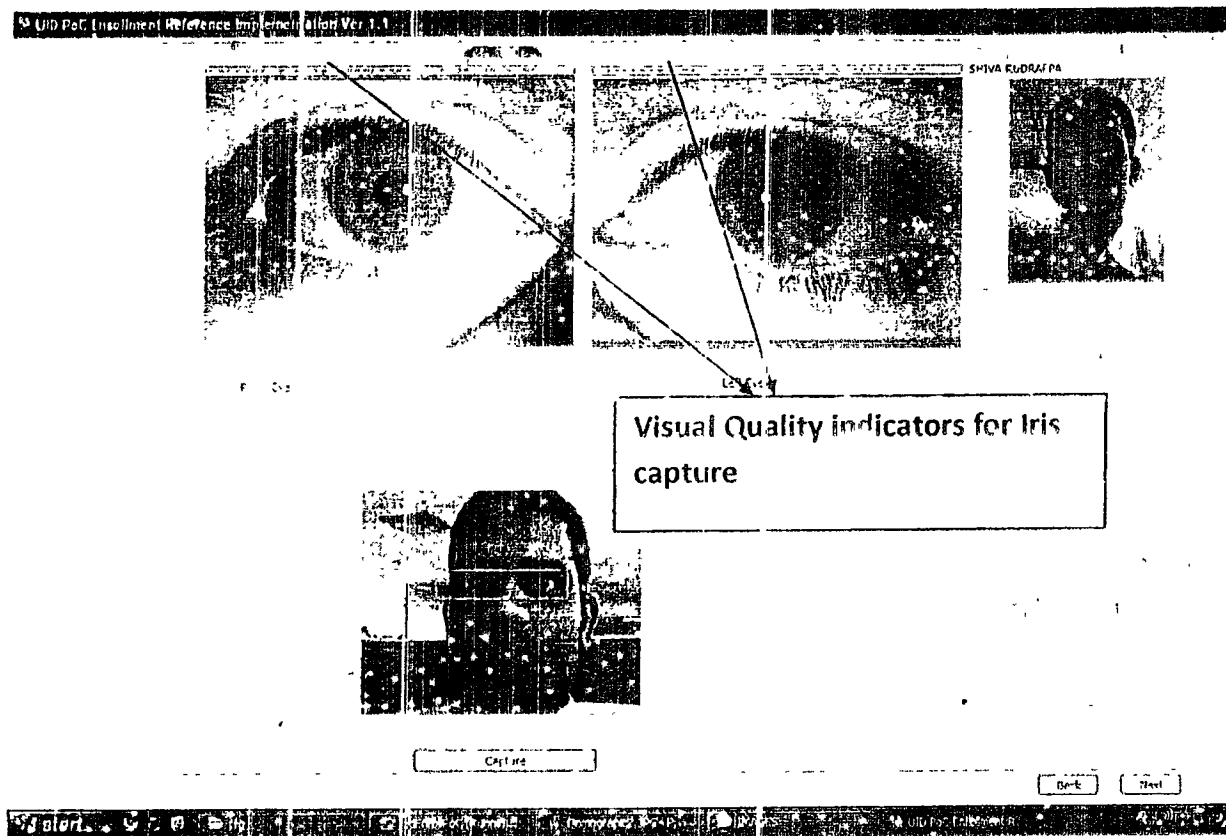
Missing Finger Indication:

Missing Eye Indication:

Clear Data Next

276
275

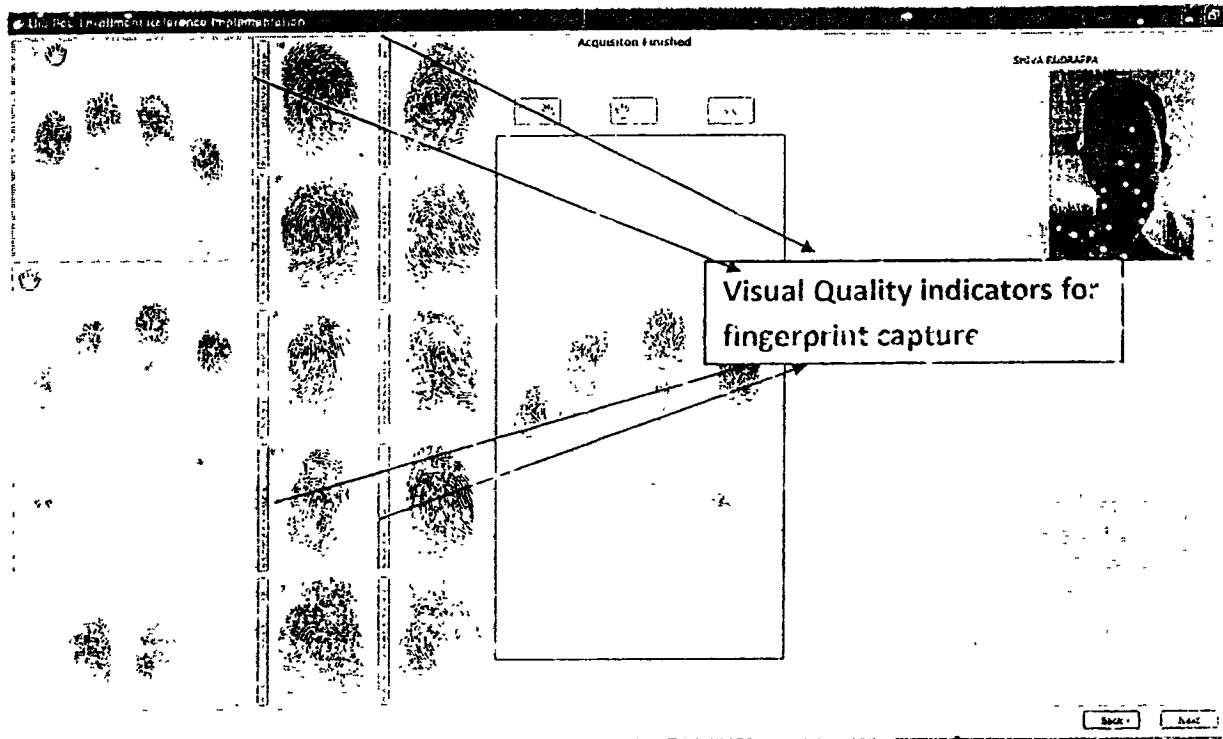
Iris Capture Screen with quality indicators highlighted



277

276

Fingerprint Capture Screen with quality indicators highlighted



2-78

467

Single Fingerprint Capture Screen

100% Fingerprint Reference Image (only for 1:1)



Back Print

279

278

Annexure 2 - Enrolment times by age and demographics

| Age | Under 20 | 20 to 30 | 30 to 40 | 40 to 50 | 50 to 60 | 60 to 70 | 70+ |
|------|----------|----------|----------|----------|----------|----------|---------|
| face | 0:00:21 | 0:00:21 | 0:00:33 | 0:00:35 | 0:00:37 | 0:00:38 | 0:00:38 |
| iris | 0:00:21 | 0:00:22 | 0:00:29 | 0:00:51 | 0:00:58 | 0:00:07 | 0:00:07 |
| slap | 0:00:15 | 0:00:52 | 0:00:48 | 0:01:45 | 0:01:53 | 0:01:56 | 0:01:56 |

Enrolment times by age

| Occupation | face | iris | slap | Total |
|-------------------|---------|---------|---------|---------|
| Entrepreneur | 0:00:27 | 0:00:53 | 0:02:16 | 0:03:36 |
| Employee | 0:00:27 | 0:00:39 | 0:01:36 | 0:02:42 |
| Daily wage earner | 0:00:25 | 0:00:46 | 0:02:08 | 0:03:19 |
| Student | 0:00:22 | 0:00:37 | 0:01:49 | 0:02:48 |
| Home worker | 0:00:27 | 0:00:59 | 0:02:04 | 0:03:29 |
| Coach | 0:00:55 | 0:00:48 | 0:01:28 | 0:03:11 |
| Farmer | 0:00:43 | 0:00:51 | 0:01:41 | 0:03:15 |
| Season Worker | 0:00:21 | 0:00:44 | 0:02:52 | 0:04:07 |
| Artisan | 0:00:22 | 0:00:42 | 0:03:20 | 0:04:24 |
| Self-employed | 0:00:23 | 0:00:39 | 0:01:52 | 0:03:34 |
| Other | 0:00:27 | 0:00:44 | 0:02:16 | 0:03:27 |
| Retiree | 0:00:28 | 0:01:40 | 0:02:08 | 0:04:16 |
| Unemployed | 0:00:24 | 0:00:37 | 0:01:18 | 0:02:39 |

Enrolment times by occupation

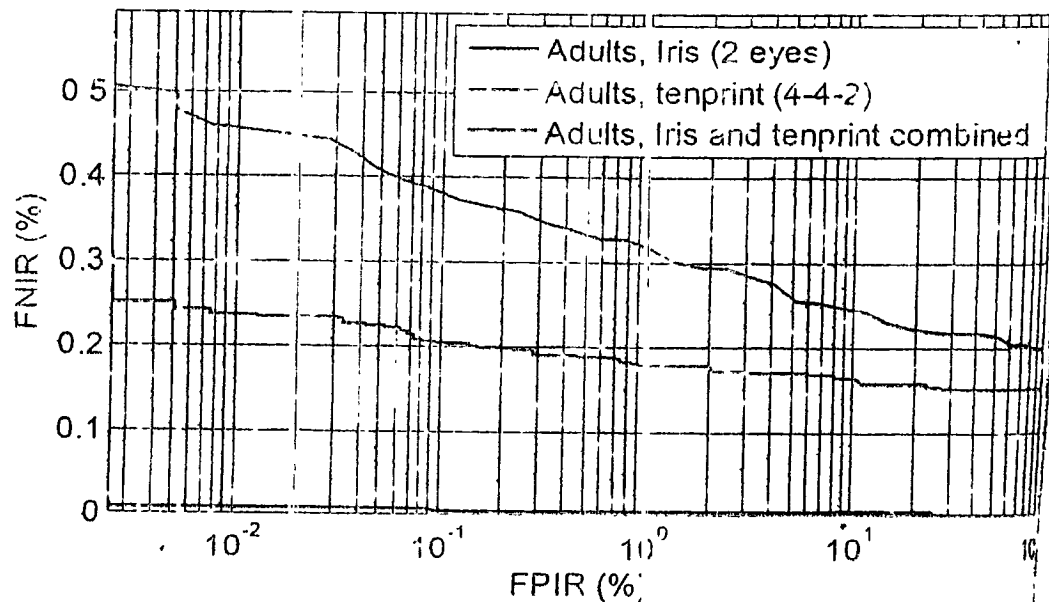
| Gender | face | iris | slap | Total |
|--------|---------|---------|---------|---------|
| Male | 0:00:30 | 0:00:48 | 0:01:50 | 0:03:08 |
| Female | 0:00:27 | 0:00:56 | 0:02:09 | 0:03:32 |

Enrolment times by gender

2.80
~~2.79~~

Annexure 3 - Biometric matching accuracy curves

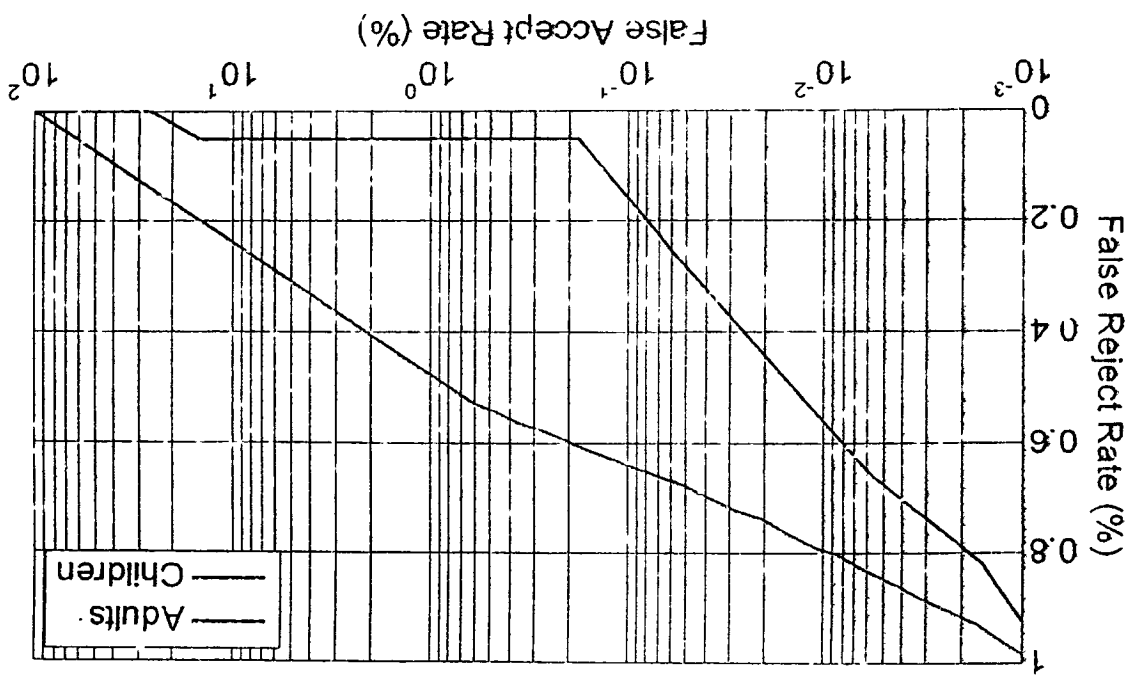
Identification ROCs(1 in 20,000) for adults



281

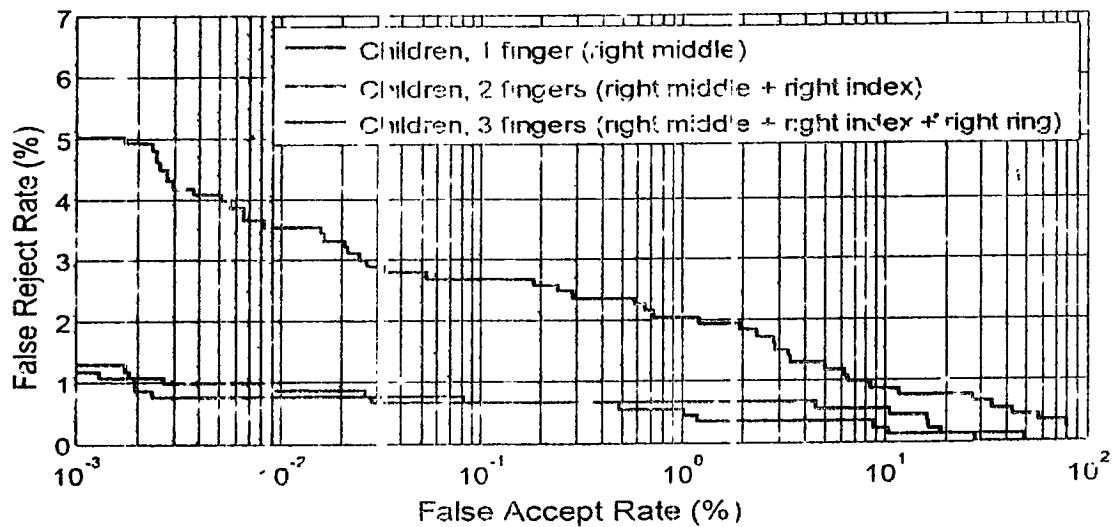
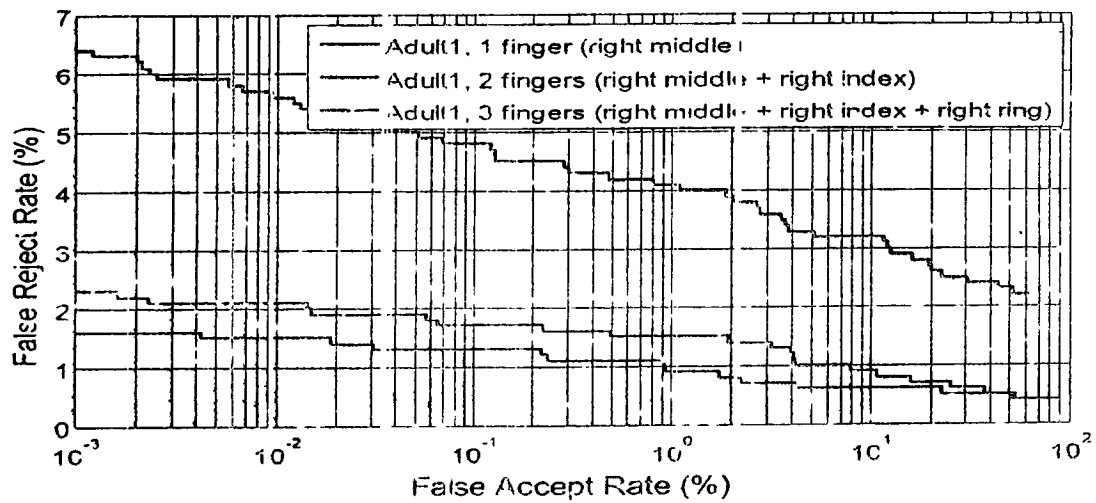
280

Iris identification ROCs (1:1) for adults and children



282
281

Verification ROC for 1,000 children and adults



True Copy
Ad

Exh - 'J'

8/6/09/12

282

28-

India's ID card scheme – drowning in a sea of false positives

by David Moss

March 2011

- UIDAI cannot possibly deliver what they promise.
- Their own figures prove it.
- If India is relying on unique identification, then India has a serious problem.

Abstract UIDAI conducted a proof of concept trial of their Aadhaar project between March and June 2010. This paper reviews their report on the trial, 'UIDAI Proof of Concept Report', published in December 2010.

First UIDAI promised that Aadhaar would deliver unique identification. Then they conducted a proof of concept trial to see if it can.

That's back to front.

"The logo for Aadhaar,
a sun in red and yellow,
with a fingerprint traced across its centre
... a new dawn of equal opportunity
for each individual"

Which quite unnecessarily exposed UIDAI to reputational risks if the trial disproved the concept. And not just UIDAI. The very senior politicians they had involved in Aadhaar could be embarrassed. The Indian people could have some legitimate questions about the proper use of public money and the competence of their government and its agencies.

The trial did disprove the concept and this paper recommends that UIDAI quickly re-establish the logical order of the Aadhaar project.

It should be made clear to politicians and the media and the public that UIDAI's promises depended on representations made to them by the biometrics industry. Those representations should be published. The biometrics companies' names should be prominently highlighted in all relevant publicity material. It is the directors of the biometrics companies whose names and faces should be well-known and should be firmly attached to all the promises of unique identification, not UIDAI's directors.

That way, if Aadhaar starts to unravel, if the sun fails to rise on the "new dawn of equal opportunity" – in short, if the argument in this paper happens to be right – the blame will be placed where it belongs and not, the wrong way round, on UIDAI.

It should be an easy decision to make, to adopt this recommendation. The alternative after all, is for UIDAI to look like the credulous dupes of some over-ambitious salesmen, dupes who wasted billions of dollars of public

283
284

money while claiming to be "pro-poor".

----- o O o -----

Introduction India has a population of something over a billion people and it is the job of the Unique Identification Authority of India (UIDAI) to enrol them all onto a population register – the CIDR or Central ID Repository – and to issue them with ID cards.

UIDAI have adopted "Aadhaar" as a brand name. Your Aadhaar (denoting foundation and support) is primarily your unique identification number, issued by UIDAI, but it is meant also to denote UIDAI-related personnel, systems, services, and products such as the ID card itself, and it is meant to inspire nationwide trust in them all and rock-solid confidence that the benefits of their project will be delivered.

----- o O o -----

The UIDAI Model According to the UIDAI Model: *"The existing patchwork of multiple databases in India provides scope to individuals to furnish different personal information to different agencies"*. India is not alone in that.

The question is, why should the CIDR database be any different from all the other databases? And the answer is, everyone hopes, biometrics: *"The UIDAI has been setup by the Government of India with a mandate to issue a unique identification number to all the residents in the country. A key requirement of the Aadhaar is to minimize/eliminate duplicate identity to improve the efficacy of the service delivery. Biometrics features are selected to be the primary mechanism for ensuring uniqueness ... Therefore, it is necessary to create a UIDAI Biometrics Centre of Competence (UBCC) that focuses on the unique challenges of UIDAI"*.

The "mission" of UBCC is: *"To design biometrics system that enables India to achieve uniqueness in the national registry"*.

The CIDR will store and use biographical data, in addition to biometrics: *"Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to minimise/eliminate duplicates in the database ..."*

But UIDAI aren't sure about the accuracy of biographical data, not in the same way they're sure (with good reason?) about biometric data. At least for the moment, the support and foundation of the CIDR is meant to be biometrics, not biographical data: *"While certain demographical information is also provided, UIDAI provides no assurance of its accuracy."*

284
255

Demographic information shall not be used for filtering during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UIDAI program".

----- o O o -----

Biometrics Should UIDAI be so sure? How reliable are the biometrics Aadhaar depends on?

Earlier reviews of the chaotic mass consumer biometrics market suggest that UIDAI have taken on an impossible task.

But now UIDAI have conducted their own, up to date, proof of concept trial and, in the *Conclusion* section of their report, they say: *"the biometric accuracy levels necessary for deduplication of all residents of India are achievable"*. This follows the claim in the *Results* section of the report that *"we can be confident that biometric matching can be used on a wider scale to realize the goal of creating unique identities"*.

In fact, those conclusions do not follow from the evidence reported. Nothing in UIDAI's surprisingly low quality report suggests that it would be feasible to prove that each electronic identity on the CIDR is unique. Not with a billion+ people on the database. Far from it, India can be confident, from the figures quoted in UIDAI's proof of concept trial report, that deduplication could never be achieved.

----- o O o -----

The sea of false positives It just takes a simple two-step argument to prove the point. Nowhere does the maths involved rise above schoolboy level.

Step 1 – uniqueness

UIDAI must create one electronic identity on the CIDR corresponding to each real person in India. Each electronic identity will include a copy of the person's fingerprints and irisprints. If UIDAI are to prove that each electronic identity is unique, then each set of biometrics must be compared to, and shown to be different from, every other set of biometrics.

UIDAI know that. As they say in the *Results* section: *"the matching analysis was done on two sets of 20,000 biometrics, for a total of 40,000. However, the number of comparisons was several orders of magnitude more than 40,000, since each set of fingerprints would be matched against every other set of fingerprints in the data set"*.

How many unique pairs of biometrics can be chosen from 40,000? Answer: $40,000 \times 39,999 / 2 = 799,980,000$. UIDAI

are right. 40,000 is a number of the order of 10^4 , whereas the number of comparisons which have to be made to prove uniqueness is of the order of 10^8 .

The population of India is of course not 40,000. More like 1.2 billion or 1.2×10^9 . So that the number of comparisons between pairs of biometrics that would need to be made to prove uniqueness is 7.2×10^{17} .

Step 2 – false positives

It would take a very long time but, in a perfect world, those 7.2×10^{17} comparisons could be performed by computer and it could be proved automatically that there are no duplicates, i.e. each electronic identity is unique.

In the real world, problems arise. UIDAI say quite rightly that they must expect the odd false positive. In other words, on occasion, it will look as though two people have the same biometrics.

There may be hundreds of reasons for that. Here are just four of them:

- The equipment used may not be entirely reliable.
- An over-worked UIDAI agent may by mistake register Mr Clark's biometrics against Mr Baker's name.
- Mr Clark may have naughtily enrolled twice, once in his real name and once as Mr Baker.
- Mr Clark and Mr Baker may genuinely be two different people who happen to have the same biometrics.

When a false positive arises, it has to be investigated by a team of human beings. It can't be resolved by computer.

How many false positives should India expect? In the *Results* section of their report UIDAI define FPIR, the false positive identification rate, and they say "we will look at the point where the FPIR (i.e. the possibility that a person is mistaken to be a different person) is 0.0025 %". At that point, UIDAI would get $2\frac{1}{2}$ false positives on average for every 100,000 comparisons.

Given that UIDAI have to make 7.2×10^{17} comparisons, how many false positives should they expect? Answer: $(7.2 \times 10^{17}) \times (2.5 \times 10^{-5}) = 1.8 \times 10^{13}$. That's 18,000,000,000,000 false positives for people to investigate and resolve.

It's just not going to happen, is it. India has got better things to do with its time than to clean up the mess left behind by today's unreliable mass consumer biometrics.

And that's the end of the argument.

To prove uniqueness, every single Indian would have to investigate and resolve 15,000 false positives. Long before they had finished, many of them would be dead, many more Indians would have been born, and the task would remain incomplete. Using UIDAI's own figures, India can be confident that the proof of uniqueness is not achievable. Not in the real world.

If any journalist asks UIDAI the question "are you sure that all the IDs on the CIDR are biometrically unique", the only truthful answer is "no".

UIDAI cannot possibly deliver what they promise. Their own figures prove it. If India is relying on unique identification, then India has a serious problem.

----- o O o -----

Feedback How many false positives would be manageable? One million? To achieve that, the FPIR would have to be 18,000,000 times smaller/better than 0.0025 percent. Is that feasible? How many more staff would UIDAI need? How much more would UIDAI have to spend on top quality biometrics equipment to make that improvement? If that is feasible, why didn't the UIDAI Biometrics Centre of Competence say so? Why did UBCC "*look at the point where the FPIR ... 0.0025 %*" and not at the point where it's 1.4×10^{-12} , which is what it would have to be to reduce the number of false positives to one million?

If the sea-of-false-positives argument above is correct, then biometrics do not provide the foundation needed for Aadhaar, the false conclusions drawn by UBCC in the proof of concept trial report impugn everyone's trust in UIDAI and no-one can be confident that the benefits of Aadhaar will be achieved.

But is the argument correct? It needs a trusted and independent third party to state their case and deliver the verdict.

Some responses to this paper have been received. More would be appreciated.

One response was to argue that the number of comparisons required to prove uniqueness would be reduced by using multi-modal biometrics. Take another look. The FPIR of 0.0025 percent used in this paper *is* the multi-modal rate. If the calculations had been based on the FPIRs for either fingerprints or irisprints singly, then the prediction would be that UIDAI would have to perform even more than 18,000,000,000,000 comparisons.

It was also suggested that biographical data used in conjunction with biometric data would reduce the number of comparisons that need to be made to prove uniqueness. That may or may not be true but it isn't what the UIDAI Model says, "*demographic information shall not be used for filtering during the de-duplication process*", as noted above, and it isn't what the proof of concept trial report says – which is that uniqueness can be proved using biometrics alone, "*the biometric accuracy levels necessary for deduplication of all residents of India are achievable*". And on that point, UIDAI are wrong.

Or so it seems. (To repeat, more feedback would be appreciated.)

----- o O o -----

13 more questions Presumably the proof of concept trial report is the work of UBCC. They have to say why the sea-of-false-positives argument is wrong, if they can. And here are 13 more questions which could do with a response from them:

1. Over the years, the suppliers of biometric technology have been caught out repeatedly making exaggerated claims for the reliability of their wares. Their marketing material is now a little less gung-ho. UIDAI's suppliers, I-1 Identity Solutions Inc. and Mugplus among others, do not claim on their websites to be able to deliver unique identification in the case of large population registers. Given the sea of false positives, how could they? So why do UIDAI claim to be able to deliver unique identification? It's easy to see why the suppliers don't object to being boosted in this way. But why do UIDAI provide this unsolicited testimonial to the historically flaky products of the mass consumer biometrics industry?
2. Should UIDAI change their name? Perhaps they should drop the word "unique" and become simply "IDAI". Or maybe they should change their name to something more like Pakistan's "NADRA", the National Database and Registration Authority. Not that NADRA seem to have brought peace, stability, social justice, universal inclusion and prosperity to Pakistan.
3. How keen will Visa and MasterCard be to proceed with their plans for biometrically verified payment services if unique identification is not available?
4. Many states of the European Union, and Pakistan, and China, and others, use biometrics for their identity management schemes. If today's mass consumer biometrics are too unreliable to prove uniqueness, are they all, like India, perhaps wasting their time and money?
5. In December 2009 UIDAI published their *Biometrics Design*

288

289

commitment to UID applications. At that stage, apparently under the influence of the US National Institute of Standards and Technology (NIST), they had high hopes of using facial geometry as a biometric. A year later, the support for facial geometry in the UIDAI Model is now tepid, at best: "Multiple modalities such as- fingerprint and iris image will be used for de-duplication. Face photograph is provided if the vendor desires to use it for de-duplication". And in the proof of concept trial, they dropped facial recognition by computer altogether. Hardly surprising. Facial geometry is traditionally the least reliable of the biometrics commonly considered. In general, people would do better to toss a coin than to rely on facial geometry. Is the International Civil Aviation Organization wasting everyone's time and money, including India's, by insisting on facial geometry being implemented in ePassports?

6. ... and are the UK, Australia and New Zealand, and Portugal wasting their time and money using so-called "smart gates" for border control at international airports? These machines rely on facial recognition. Does India intend to install them?

7. UIDAI's identification results (*Annexure 3*, p.30) are based on 20,000 people chosen from the 60,000 who attended two biometric enrolment sessions. What do the results for all 60,000 look like? Why were the full results not published? How were the 20,000 chosen? What was wrong with the other 40,000? Why don't UIDAI report the deduplication statistics for the one million people now enrolled on the CIDR, instead of a paltry 20,000 of them?

8. Is a field trial of 20,000 big enough to tell India what to expect when it comes to 1.2 billion people?

9. UIDAI are going to need a lot of different staff using a lot of different biometrics equipment in a lot of different urban and rural locations - how feasible is it to keep the FPIR as low as 0.0025 percent?

10. Most of the participants in the proof of concept trial were adults. UIDAI's report is not precise on this point, but it looks as though the results for children are based overwhelmingly on a sample taken from just one school. If that is the case, they can tell India so little, why do UIDAI bother to publish the children's results in the trial report?

11. Why don't Visa and MasterCard rely on biometrically verified payments anywhere in Europe and the US? If they're not good enough for Europe and the US, why should they be acceptable in India?

12. The US company Pay By Touch tried to promote biometrically verified payment services. They went bust. Have

289

290

UIDAI considered this warning?

13. CIIAC, the body representing 1,800 business schools in 110 countries, dropped fingerprinting as a way of verifying identity after a two-year trial. If the business schools don't recommend the technology, why do UIDAI recommend it?

----- o O o -----

Identification v. verification This paper concentrates on the problems of *identification*, i.e. proving that each record on the CIDR is unique.

Some attention must be paid to the separate problems of *verification*, i.e. proving that your biometrics are the same as the biometrics on the ID card/passport that you are using to cross a state border, for example, or to register with a doctor to obtain state healthcare or to prove your right to work in India.

When it comes to verifying identity, there is a trade-off between false reject rates and false accept rates, they are inversely proportional. The false accept rate must be low to reduce the probability of impostors defrauding the state and the banks. But that tends to push up the false reject rate, more people get wrongly told by a computer that they are not themselves. And when that happens, they can't cross the border or register with the doctor or get the new job.

The *iris verification ROCs (1:1) for adults and children* graph in the proof of concept trial report (*Annexure 3*, p.31) should probably be labelled "Iris verification ROCs (1:1) for adults and children" UBCC have some way to go.

It is impossible to tell from UIDAI's report what the level of false rejection in Aadhaar is. It could be very low. It could be just over 6 percent (*Annexure 3*, p.32). It could be anything - *one study found in the UK found a false reject rate for fingerprints, using L-1 Identity Solutions technology, of about 20 percent.*

But if the entitlement to public services depends on the biometric verification of identity, and if 6 percent of the population find themselves denied their entitlement as a result, that's 72 million excluded people. They will not be pleased. Neither will Visa and MasterCard be pleased, if they find that they lose 72 million customers because biometric verification is still too unreliable.

72 million rioting people have a way of making their anger and disappointment felt. The result may be that biometrics are no use to India and that all the money spent on Aadhaar is

wasted.

----- o O o -----

Back to front The proper conclusion from UIDAI's proof of concept trial seems to be that the concept is not proven, the system design is a failure, its hypothesis is wrong, unique identification is not achievable. Ask any 16 year-old studying science (any *logical* 16 year-old, come to think of it, not just science students), that should be the signal to halt Aadhaar and think again.

The proof of concept trial report reviewed here is a poor support for Indian confidence, it provides no foundation for trust in UIDAI and it diminishes the Aadhaar brand. The trial results are the opposite of the stated conclusions. UBCC need to raise their game before they conduct their next biometrics trial.

The figures show that unique identification is not possible, the report states that it is. The proof of concept trial is a failure, the Aadhaar project proceeds nevertheless. It's all back to front. Why?

Because UIDAI's approach to biometrics is back to front.

First UIDAI assumed that today's mass consumer biometrics technology is reliable enough to deliver unique identification and adequate verification. They made all their plans accordingly. They hired staff. They contracted with registrars and enrolment agencies and introducers and authenticators (as per the UIDAI Model). They paraded the most senior politicians in the land to give the project their backing. They briefed the press and they ran a nationwide publicity campaign. Global, even. All the while, they were making promises, raising expectations, committing themselves. A lot of hope, wishful thinking, the best of intentions, sackloads of public money, the benefits would be monumental. Then, and only then, they conducted a trial to test the feasibility of Aadhaar. That's the wrong way round.

As it happens, the UK made the same mistake. For years, between 2002 and 2010, the Home Office were in the undignified position of being quite unable to answer probing questions, whether posed by critics or supporters, about the proposed UK ID card scheme. The facts simply don't support the claims the Home Office was



Damian Green MP feeding disk drives from the failed UK ID card scheme and the credibility of the Home Office into an individual's shadow

291

292

making – see for example their document "safeguarding

Photograph: SA Matheson/Guardian

identity' – about being able to "lock" people to a single identity (para.3.29) and their fatuous promise that ID cards would "make life easier" (para.2.1). Public money was wasted on a pipe dream.

There were many problems with the UK scheme. Not just biometrics. But biometrics is the easiest problem to understand and to discuss objectively and on which to reach an agreed decision, it's quantifiable, there are no difficult value judgements to make, it's just technology. And not a very good technology – whenever there is a large-scale field trial, as opposed to the mere computer modelling exercises favoured by NIST, mass consumer biometrics prove to be too unreliable for the ID card schemes that depend on them.

By the time the stillborn scheme was finally cancelled, the Home Office had lost all credibility, it was totally demoralised and it is now excluded from discussions of the UK's new, and still unspecified, Digital Delivery Identity Assurance project.

----- o O o -----

Deduping UIDAI If UIDAI wish to avoid the same fate – ridicule, disgrace, ostracisation, ... – they had better display a lot more dignity than the UK Home Office did for eight years.

The danger exists that, having given their unsolicited testimonials to the biometrics industry and its unreliable products, UIDAI will be left to clean up the expensive mess left in India as best they can when Aadhaar is cancelled, while the biometrics industry road-show moves on to the next country and repeats the trick.

UIDAI need to make it clear to politicians and the media and the public that the magical claims made for biometric identification and verification were hypothetical. They have been proved to be wrong. *And that's the biometrics industry's problem, not UIDAI's.*

There are any number of news items in the media like the following article by Amruta Byatnal published in *The Hindu* of 29 September 2010 ...

Tembhli becomes first Aadhar village in India

Ranjana Sonawne 782474317884 With this number, Ranjana has become the first Indian to get the UID (Unique Identification) Prime Minister Manmohan Singh and United Progressive Alliance Chairperson Sonia Gandhi launched the Aadhar project ...

292
293



Prime Minister Manmohan Singh and UPA chairperson Sonia Gandhi present the Unique Identification card to a tribal woman in Tembhli, Maharashtra

The Unique Identification Authority of India (UIDAI) chief, Nandan Nilekani, Maharashtra Chief Minister Ashok Chavan, Deputy Chief Minister Chhagan Bhujbal, Maharashtra Governor K. Shankaranarayanan, Planning Commission Deputy Chairman Montek Singh Ahluwalia were also present at the inauguration function

Stating that the UID will help people in 'all fields,' Ms. Gandhi stated: "Our idea is to not just focus on development, but to bring about inclusive growth amongst our people. This scheme will make sure people will get what they deserve"

Dr. Singh congratulated the UIDAI and said, "UID will help the hundreds of people in India, whose pride was hurt for so many years because of the lack of an identity. This will be their source of recognition from now on."

Making life easy

He clarified that the UID number will now enable them to open bank accounts without any hassle, get ration anywhere in the country and to get job cards, among other facilities.

... the recommendation in this paper is that UIDAI should ensure that a lot of news items like the following *mock-up* are published in addition. And journalists should lose no opportunity to ask the directors of the companies supplying biometric technology to UIDAI to confirm that it is feasible to prove that each electronic identity on the CIDR is biometrically unique:

Aadhaar: biometrics companies provide copper bottom guarantee



Jean-Paul Herteman, CEO of Morpho, the company that owns the Aadhaar ID card scheme

Leaders of two of the biggest blue-chip companies providing biometrics technology to India's 1.2 billion Aadhaar ID card scheme joined together today to congratulate both Prime



Robert V. LaPenta, Chairman, President and CEO of L. Identity Solutions, Inc. (soon to be part of Morpho)

Minister Manmohan Singh on his vision and Unique Identification Authority of India (UIDAI)

294

293

chief Nandan Nilekani on his energy. The fingerprint and iris know-how of Morpho and L-1 Identity Solutions lies at the heart of Aadhaar. The ability to provide a unique identity to every resident of India depends on the uniqueness of their biometrics, as recorded by Mr Herteman's high-tech equipment and Mr LaPenta's.

Scientifically proven – the power of technology

"This has never been done before", they said, "anywhere in the world. UIDAI need our skillset to be 100 percent reliable, we are proud to be underwriting the biggest social project on the planet and we thank Mr Nilekani for giving us the opportunity to help. In years to come, India will be transformed by Aadhaar into a 21st century powerhouse and that will indubitably be thanks to our biometrics and to Prime Minister Singh's faith in our companies".

----- o O o -----

Pro-poor approach According to the UIDAI Model, India is adopting a pro-poor approach: *"The UIDAI envisions full enrolment of the residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the Authority plans to partner with in its first phase ... will help bring large number of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor"*.

The poor are not helped by UIDAI pretending that a technology works when it doesn't. Who is?

Updates:

18 March 2011: Now UIDAI quoted up pilot test results to press forward with IDP scheme

David Moss spent eight years campaigning against the Home Office's ID card scheme RIP. Whitehall haven't given up yet – a national identity assurance service has appeared in their G Cloud Programme. We shall see.

© 2011 Business Consultancy Services Ltd
on behalf of Dematerialised World

THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL, 2010

ARRANGEMENT OF CLAUSES

CHAPTER I

PRELIMINARY

CLAUSES

1. Short title, extent and commencement.
2. Definitions.

CHAPTER II

AADHAAR NUMBERS

3. Aadhaar number.
4. Properties of aadhaar number.
5. Authentication of aadhaar number.
6. Aadhaar number not evidence of citizenship or domicile, etc.
7. Central Identities Data Repository.
8. Updation of certain information.
9. Prohibition on requiring certain information.
10. Special measures for issuance of aadhaar number to certain categories of persons.

CHAPTER III

NATIONAL IDENTIFICATION AUTHORITY OF INDIA

11. Establishment of Authority.
12. Composition of Authority.
13. Qualifications for appointment of Chairperson and Members of Authority.
14. Term of office and other conditions of service of Chairperson and Members.
15. Removal of Chairperson and Members.
16. Restrictions on Chairperson or Members on employment after cessation of office.
17. Functions of Chairperson.
18. Meetings.
19. Vacancies, etc. not to invalidate proceedings of Authority.
20. Officers and other employees of Authority.
21. Functions of chief executive officer of Authority.
22. Transfer of assets, liabilities of Authority.
23. Powers and functions of Authority.

CHAPTER IV

GRANTS, ACCOUNTS AND AUDIT AND ANNUAL REPORT

24. Grants by Central Government.
25. Other fees and revenue.
26. Accounts and audit.
27. Returns and annual report, etc.

295
296

(u)

CHAPTER V

IDENTITY REVIEW COMMITTEE

CLAUSES

28. Review Committee.
29. Functions of Review Committee.

CHAPTER VI

PROTECTION OF INFORMATION

30. Security and confidentiality of information.
31. Alteration of demographic information or biometric information.
32. Access to own information and records of requests for authentication.
33. Disclosure of information in certain cases.

CHAPTER VII

OFFENCES AND PENALTIES

34. Penalty for impersonation at time of enrolment.
35. Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information.
36. Penalty for impersonation.
37. Penalty for disclosing identity information.
38. Penalty for unauthorised access to the Central Identities Data Repository.
39. Penalty for tampering with data in Central Identities Data Repository.
40. Penalty for manipulating biometric information.
41. General penalty.
42. Offences by companies.
43. Act to apply for offence or contravention committed outside India.
44. Power to investigate offences.
45. Penalties not to interfere with other punishments.
46. Cognizance of offences.

CHAPTER VIII

MISCELLANEOUS

47. Power of Central Government to supersede Authority.
48. Members, officers, etc., to be public servants.
49. Power of Central Government to issue directions.
50. Delegation.
51. Protection of action taken in good faith.
52. Power of Central Government to make rules.
53. Power of Authority to make regulations.
54. Laying of rules and regulations before Parliament.
55. Application of other laws not barred.
56. Power to remove difficulties.
57. Savings.

297
296

TO BE INTRODUCED IN THE RAJYA SABHA

Bill No. LXXV of 2010

THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA
BILL, 2010

A
BILL

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 and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Sixty-first Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

1. (1) This Act may be called the National Identification Authority of India Act, 2010.

5 (2) It shall extend to the whole of India except the State of Jammu and Kashmir and save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

Short title,
extent and
commencement

(3) It shall come into force 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 and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision

Definitions

2. In this Act, unless the context otherwise requires,—

(a) "aadhaar number" means the identification number issued to an individual under sub-section (2) of section 3.

(b) "aadhaar number holder" means an individual who has been issued an aadhaar number under this Act,

(c) "authentication" means the process wherein aadhaar 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

(d) "Authority" means the National Identification Authority of India established under sub-section (1) of section 11

(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 centralised database in one or more locations containing all aadhaar numbers issued to aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto:

(g) "Chairperson" means the Chairperson of the Authority appointed under section 12:

(h) "demographic information" includes information relating to the name, age, gender and address of an individual (other than race, religion, caste, tribe, ethnicity, language, income or health) and such other information as may be specified in the regulations for the purpose of issuing an aadhaar number.

(i) "enrolling agency" means an agency appointed by the Authority or by the Registrars, as the case may be, for collecting information under this Act:

(j) "enrolment" means such process, as may be specified by regulations, to collect demographic information and biometric information from individuals by the enrolling agencies for the purpose of issuing of aadhaar number to such individuals under this Act;

(k) "identity information" in respect of an individual means biometric information, demographic information and aadhaar number of such individuals:

(l) "Member" includes the Chairperson and a part-time Member of the Authority appointed under section 12.

(m) "notification" means a notification published in the Official Gazette and the expression "notified" with its cognate meanings and grammatical variations shall be construed accordingly;

(n) "prescribed" means prescribed by rules made under this Act;

(o) "Registrar" means any entity authorised or recognised by the Authority for the purpose of enrolling the individuals under this Act;

(p) "regulations" means the regulations made by the Authority under this Act;

(q) "resident" means an individual usually residing in a village or rural area or town or ward or demarcated area (demarcated by the Registrar General of Citizen Registration) within a ward in a town or urban area in India;

(r) "Review Committee" means the Identification Review Committee constituted under sub-section (1) of section 28.

299
298

CHAPTER II

AADHAAR NUMBERS

| | | |
|----|--|---|
| 5 | 3. (1) Every resident shall be entitled to obtain an aadhaar number on providing of his demographic information and biometric information to the Authority in such manner as may be specified by regulations: | Aadhaar number |
| | Provided that the Central Government may, from time to time, notify such other category or individuals who may be entitled to obtain an aadhaar number. | |
| 10 | (2) On receipt of the demographic information and biometric information under sub-section (1), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an aadhaar number to such resident | |
| | 4. (1) An aadhaar number, issued to an individual shall not be re-assigned to any other individual | Properties of aadhaar number |
| | (2) An aadhaar number shall be a random number and bear no attributes or identity data or part thereof, relating to the aadhaar number holder | |
| 15 | (3) An aadhaar number shall, subject to authentication, be accepted as proof of identity of the aadhaar number holder. | |
| 3) | 5. (1) The Authority shall perform authentication of the aadhaar number of a aadhaar 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 | Authentication of aadhaar number |
| | (2) The Authority shall respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic information and biometric information | |
| 25 | 6. The aadhaar number or the authentication thereof shall not, by itself, confer any right of or be proof of citizenship or domicile in respect of an aadhaar number holder. | Aadhaar number not evidence of citizenship or domicile, etc |
| | 7. The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations | Central Identities Data Repository. |
| 30 | 8. The Authority may require the aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations so as to ensure continued accuracy of their information in the Central Identities Data Repository | Update or certain information |
| | 9. The Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health | Prohibition on requiring certain information. |
| 35 | 10. The Authority shall take special measures to issue aadhaar number to women, children, senior citizens, persons with disability, migrant unskilled and unorganised 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. | Special measures for issuance of aadhaar number to certain categories of persons. |

CHAPTER III

NATIONAL IDENTIFICATION AUTHORITY OF INDIA

| | | |
|----|--|----------------------------|
| 40 | 11. (1) 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. | Establishment of Authority |
|----|--|----------------------------|

300
299

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

(3) The head office of the Authority shall be in the National Capital Region referred to in clause (f) of section 2 of the National Capital Region Planning Board Act, 1985. 5
2 of 1985

(4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

Composition
of Authority

12. The Authority shall consist of a Chairperson and two part-time Members to be appointed by the Central Government. 10

Qualifications
for appointment of Chair-
person and
Members of
Authority

13. The Chairperson and Members of the Authority shall be persons of ability, integrity and outstanding calibre having experience and knowledge in the matters relating to technology, governance, law, development, economics, finance, management, public affairs or administration.

Term of office
and other
conditions of
service of
Chairperson
and Members.

14. (1) The Chairperson and the Members appointed under this Act shall hold office for a term of three years from the date on which they assume office and shall be eligible for reappointment. 15

Provided that no person shall hold office as a Chairperson or Member after he has attained the age of sixty-five years.

Provided further that the Chairperson of the Unique Identification Authority of India appointed before the commencement of this Act by notification A-43011/02/2009-Admin.1 (Vol.II) dated the 2nd July, 2009 shall continue as a Chairperson of the Authority under this Act for the term for which he had been appointed. 20

(2) The Chairperson and every Member shall, before entering upon their office, make and subscribe to, an oath of office and of secrecy, in such form and in such manner and before such Authority as may be prescribed. 25

(3) Notwithstanding anything contained in sub-section (1), the Chairperson or Member may—

(a) relinquish his office, by giving in writing to the Central Government, a notice of not less than thirty days; or 30

(b) be removed from his office in accordance with the provisions of section 15.

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

(5) The salaries and allowances payable to, and the other terms and conditions of service of, the Chairperson and allowances or remuneration payable to part-time Members shall be such as may be prescribed. 35

Provided that the salary, allowances and the other terms and conditions of service of the Chairperson shall not be varied to his disadvantage after his appointment.

Removal of
Chairperson
and Members.

15. (1) The Central Government may remove from office the Chairperson, or a Member, who— 40

(a) is, or at any time has been adjudged as an 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, 45

(d) has acquired such financial or 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 the Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

301
300

(2) The Chairperson or a 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.

16. The Chairperson or a Member, ceasing to hold office as such, shall not, without previous approval of the Central Government,—

Restrictions on
Chairperson or
Members on
employment
after cessation
of office

(a) 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.

30 Provided that nothing contained in this clause shall apply to any employment under the Central Government or a State Government or local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in section 617 of the Companies Act 1956.

45 (b) act, for or on behalf of any person or organisation in connection with any specific proceeding or transaction or negotiation or a case to which the Authority is a party and with respect to which the Chairperson or such Member had, before cessation of office, acted for or provided advice to, the Authority.

30 (c) give advice to any person using information which was obtained in his capacity as the Chairperson or a Member and being unavailable to or not being able to be made available to the public,

(d) enter, for a period of three years from his last day in office, into a contract of service with, accept an appointment to a board of directors of, or accept an offer of employment with, an entity with which he had direct and significant official dealings during his term of office as such.

25 17. The Chairperson shall have powers of general superintendence, direction in the conduct of the affairs of the Authority and he shall, in addition to presiding over the meetings of the Authority, and without prejudice to any of the provisions of this Act, exercise and discharge such other powers and functions of the Authority as may be prescribed.

Functions of
Chairperson

30 18. (1) The Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be specified by regulations.

Meetings.

(2) The Chairperson, or, if for any reason, he is unable to attend a meeting of the Authority, the senior most Member shall preside over the meetings of the Authority.

35 (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes by the Members present and voting and in the event of an equality of votes, the Chairperson or in his absence the Member presiding over shall have a second or casting vote.

40 (4) All decisions of the Authority shall be authenticated by the signature of the Chairperson or any other Member authorised by the Authority in this behalf.

45 (5) If any Member, who is a director of a company and who as such director, has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority, he shall, as soon as possible after relevant circumstances have come to his knowledge, disclose the nature of his interest at such meeting and such disclosure shall be recorded in the proceedings of the Authority, and the Member shall not take part in any deliberation or decision of the Authority with respect to that matter.

19. No act or proceeding of the Authority shall be invalid merely by reason of—

Vacancies,
etc. not to
invalidate
proceedings
of Authority

(a) any vacancy in, or any defect in the constitution of, the Authority;

(b) any defect in the appointment of a person as a Member of the Authority; or

(c) any irregularity in the procedure of the Authority not affecting the merits of the case.

Officers and
other
employees of
Authority

20. (1) 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.

(2) The Authority may, with the approval of the Central Government, determine the number, nature and categories of other officers and employees required to the Authority in the discharge of its functions.

(3) The salaries and allowances payable to, and the other terms and conditions of service of, the chief executive officer and other officers and other employees of the Authority shall be such as may be specified by regulations with the approval of the Central Government.

Functions of
chief executive
officer of
Authority.

21. (1) The chief executive officer shall be the legal representative of the Authority and shall be responsible for—

(a) the day-to-day administration of the Authority,

(b) implementing the work programmes and decisions adopted by the Authority;

(c) drawing up of proposal for the Authority's work programme;

(d) the preparation of the statement of revenue and expenditure and the execution of the budget of the Authority.

(2) Every year, the chief executive officer shall submit to the Authority for approval—

(a) a general report covering all the activities of the Authority in the previous year;

(b) programmes of work;

(c) the annual accounts for the previous year, and

(d) the budget for the coming year.

(3) The chief executive officer shall have administrative control over the officers and other employees of the Authority.

Transfer
of assets,
liabilities of
Authority.

22. On and from the establishment of the Authority —

(1) 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.

Explanation. — The assets of such Unique Identification Authority of India shall be deemed to include all rights and powers, and all properties, whether movable or immovable, including, in particular, cash balances, deposits and all other interests and rights in, or arising out of, such properties as may be in the possession of such Unique Identification Authority of India and all books of account and other documents relating to the same; and liabilities shall be deemed to include all debts, liabilities and obligations of whatever kind,

(2) without prejudice to the provisions of sub-section (1), all data and information collected during enrolment, all details of authentication performed, debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for such Unique Identification Authority of India immediately before that day, for or in connection with the purpose of the said Unique Identification Authority of India, shall be deemed to have been incurred, entered into or engaged to be done by, with or for, the Authority,

(3) all sums of money due to the Unique Identification Authority of India immediately before that day, shall be deemed to be due to the Authority, and

(4) all suits and other legal proceedings instituted or which could have been instituted by or against such Unique Identification Authority of India immediately before that day may be continued or may be instituted by or against the Authority.

23. (1) The Authority shall develop the policy, procedure and systems for issuing aadhaar numbers to residents and perform authentication thereof under this Act.

Powers and
functions of
Authority

(2) 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,—

- (a) specifying, by regulation, demographic information and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof;
- (b) collecting demographic information and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations;
- (c) appointing or one or more entities to operate the Central Identities Data Repository;
- (d) generating and assigning aadhaar numbers to individuals;
- (e) performing authentication of the aadhaar numbers;
- (f) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;
- (g) omitting and deactivating of an aadhaar number and information relating thereto in such manner as may be specified by regulations;
- (h) specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations;
- (i) specifying, by regulation, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;
- (j) establishing, operating and maintaining of the Central Identities Data Repository;
- (k) sharing, in such manner as may be specified by regulations, the information of aadhaar 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;
- (l) calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;
- (m) specifying, by regulation, various processes relating to data management security protocols and other technology safeguards under this Act;
- (n) specifying, by regulation, the conditions and procedures for issuance of new aadhaar number to existing aadhaar number holder;
- (o) levy and collect the fees or authorise the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;
- (p) appoint such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;
- (q) promote research and development for advancement in biometrics and related areas, including usage and applications of aadhaar numbers through appropriate mechanisms;
- (r) specifying, by regulation, the policies and practices for Registrars, enrolling agencies and other service providers.

303
304

(a) setting up facilitation centres and grievance redressal mechanisms for redressal of grievances of residents, Registrars enrolling agencies and other service providers;

(c) such other powers and functions as may be prescribed.

(3) The Authority may,—

(a) enter into a Memorandum of Understanding or agreement as the case may be, with Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or performing authentication;

(b) by notification, appoint such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto,

as may be necessary for the purposes of this Act

(4) The Authority may engage such consultants, advisers and other persons as may be required for efficient discharge of its functions under this Act on such allowances or remuneration and terms and conditions as may be specified by regulations.

CHAPTER IV

GRANTS, ACCOUNTS AND AUDIT AND ANNUAL REPORT

Grants by
Central
Government

24. 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 utilised for the purposes of this Act

Other fees and
revenue

25. The fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India and the entire amount so credited be transferred to the Authority.

Accounts and
audit.

26. (1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India

(2) The accounts of the Authority shall be audited annually by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Authority to the Comptroller and Auditor-General.

(3) The Comptroller and Auditor-General and any person appointed by him in connection with the audit of the accounts of the Authority under this Act shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has in connection with the audit of Government accounts, and in particular, shall have the right to demand production of books, accounts, connected vouchers and other documents and papers and to inspect any of the offices of the Authority.

(4) The accounts of the Authority, as certified by the Comptroller and Auditor-General or any other person appointed by him in this behalf, together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the audit report to be laid, as soon as may be after it is received, before each House of Parliament.

Returns and
annual report,
etc

27. (1) The Authority shall furnish to the Central Government at such time and in such form and 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.

(2) The Authority shall prepare, once in every year, and in such form and manner and at such time as may be prescribed, an annual report giving—

(a) a description of all the activities of the Authority for the previous years,

(b) the annual accounts for the previous year; and

(c) the programmes of work for coming year.

305
304

(3) A copy of the report received under sub-section (2) shall be laid by the Central Government, as soon as may be after it is received, before each House of Parliament.

CHAPTER V

IDENTITY REVIEW COMMITTEE

5 28. (1) The Central Government may, by notification, constitute the Identity Review Committee to discharge functions specified under sub-section (1) of section 29 in respect of any matter connected with the usage of the aadhaar numbers. Review Committee

(2) The Review Committee shall consist of three members (one of whom shall be chairperson designated as such by the Central Government) who are persons of eminence, ability, integrity and standing in public life having knowledge and experience in the fields of technology, law, administration and governance, social service, journalism, management or social sciences.

(3) The members of the Review Committee shall be appointed by the Central Government on the recommendations of a committee consisting of—

- 15 (a) the Prime Minister, who shall be the Chairperson of the committee;
(b) the Leader of Opposition in the Lok Sabha; and
(c) a Union Cabinet Minister to be nominated by the Prime Minister.

Explanation — For the removal of doubts, it is hereby declared that where the Leader of the Opposition in the House of the People has not been recognised as such, the Leader of the single largest group in Opposition or the Government in the House of the People shall be deemed to be the Leader of the Opposition.

(4) The member of the Review Committee shall not be a Member of Parliament or Member of the Legislature of any State or Union territory, as the case may be, or a member of any political party.

25 (5) 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 reappointment.

(6) The Central Government may by order remove from office any member of the Review Committee, who—

- 30 (a) is, or at any time has been adjudged as an 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
35 (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;

Provided that a Member shall not be removed under clause (d) or clause (e) unless he has been given a reasonable opportunity of being heard in the matter.

40 29. (1) The Review Committee shall ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government. Functions of Review Committee

(2) The manner of preparation of the report referred to in sub-section (1) shall be such as may be determined by the Review Committee.

45 (3) A 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.

10
CHAPTER VI

PROTECTION OF INFORMATION

Security and confidentiality of information

30. (1) The Authority shall ensure the security and confidentiality of identity information and authentication records of individuals

(2) 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 unauthorised access or use or unauthorised disclosure thereof

(3) Notwithstanding anything contained in any other law and 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 shall not, whether during his service as such or thereafter, reveal any information stored in the Central Identities Data Repository to any person

Provided that an aadhaar number holder may request the Authority to provide access to his identity information in such manner as may be specified by regulations

Alteration of demographic information or biometric information.

31. (1) In case any demographic information relating to an aadhaar number holder is found incorrect or changes subsequently, the aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(2) In case any biometric information of aadhaar number holder is lost or changes subsequently for any reason, the aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(3) 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 aadhaar number holder and intimate such alteration to the concerned aadhaar number holder.

Access to own information and records of requests for authentication.

32. (1) The Authority shall maintain details of every request for authentication of the identity of every aadhaar number holder and the response provided thereon by it in such manner and for such time as may be specified by regulations

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

Disclosure of information in certain cases

33. Nothing contained in sub-section (3) of section 30 shall apply in respect of—

(a) any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or

(b) any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorised in this behalf by an order of the Central Government.

CHAPTER VII

OFFENCES AND PENALTIES

Penalty for impersonation at time of enrolment

34. Whoever impersonates or attempts 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.

35. Whoever, with the intention of causing harm or mischief to a aadhaar number holder, or with the intention of appropriating the identity of a aadhaar number holder changes or attempts to change any demographic information or biometric information of a aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, 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. Penalty for impersonation of aadhaar number holder by changing demographic information or biometric information
36. Whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorised 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. Penalty for impersonation
37. Whoever intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised 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. Penalty for disclosing identity information
38. Whoever, not being authorized by the Authority, intentionally,—
- (a) accesses or secures access to the Central Identities Data Repository; or
 - (b) downloads, copies or extracts any data from the Central Identities Data Repository or stored in any removable storage medium; or
 - (c) introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository; or
 - (d) damages or causes to be damaged the data in the Central Identities Data Repository; or
 - (e) disrupts or causes disruption of the access to the Central Identities Data Repository; or
 - (f) denies or causes a denial of access to any person who is authorised to access the Central Identities Data Repository; or
 - (g) provides any assistance to any person to do any of the acts aforementioned,
- or
- (h) destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or effects injuriously by any means; or
 - (i) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage,
- shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which shall not be less than one crore rupees. Penalty for unauthorised access to the Central Identities Data Repository
- Explanation* — For the purposes of this section, the expressions "computer contaminant", "computer virus" and "damage" shall have the meanings respectively assigned to them in the *Explanation* to section 43 of the Information Technology Act, 2000. Penalty for tampering with data in Central Identities Data Repository.
39. Whoever, not being authorised by the Authority, uses or tampers with the data in the Central Identities Data Repository or in any removable storage medium with the intent of modifying information relating to aadhaar 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. Penalty for manipulating biometric information
40. Whoever gives or attempts to give any biometric information which does not pertain to him for the purpose of getting an aadhaar number or authentication or updating his information, 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 with both.

General
penalty.

41. Whoever commits an offence under this Act for which no penalty is provided elsewhere than in this section, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Offences by
companies.

42. (1) 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:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence

(2) Notwithstanding anything contained in sub-section (1), 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

Explanation — For the purposes of this section—

(a) "company" means any body corporate and includes a firm or other association of individuals; and

(b) "director", in relation to a firm, means a partner in the firm

Act to apply
for offence or
contravention
committed
outside India

43. (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.

(2) For the purposes 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 Central Identities Data Repository

Power to
investigate
offences.

44. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector of Police shall investigate any offence under this Act.

Penalties not
to interfere
with other
punishments

45. 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.

Cognizance of
offences.

46. (1) 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 authorised by it.

(2) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act

CHAPTER VIII

MISCELLANEOUS

Power of
Central
Government
to supersede
Authority

47. (1) If, at 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

307
308

5 (h) 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

(i) 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 10 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.

15 (2) Upon the publication of a notification under sub-section (1) superseding the Authority,—

(a) the Chairperson and other members shall, as from the date of supersession, vacate their offices as such,

20 (b) all the powers, functions and duties which may, by or under the provisions of this Act, be exercised or discharged by or on behalf of the Authority shall, until the Authority is reconstituted under sub-section (3), be exercised and discharged by the person or persons referred to in sub-section (1), and

(c) all properties owned or controlled by the Authority shall, until the Authority is reconstituted under sub-section (3), vest in the Central Government.

25 (3) On or before the expiration of the period of supersession specified in the notification issued under sub-section (1), the Central Government shall reconstitute the Authority by a fresh appointment of its Chairperson and other members and in such case any person who had vacated his office under clause (a) of sub-section (2) shall not be deemed to be disqualified for reappointment.

30 (4) The Central Government shall cause a copy of the notification issued under sub-section (1) and a full report of any action taken under this section and the circumstances leading to such action to be laid before each House of Parliament at the earliest

48. 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

48 of 1360 35

Members, officers, etc. to be public servants

49. 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

Power of Central Government to issue directions

40 Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

(2) The decision of the Central Government, whether a question is one of policy or not, shall be final

50. The Authority may, by general or special order in writing, delegate to any Member, officer of the Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 53) as it may deem necessary.

45

Delegation

10
89

Protection of
action taken
in good faith.

51. 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

Power of
Central
Government
to make rules.

52. (1) The Central Government may, by notification, make rules to carry out the provisions of this Act. 5

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely —

(a) the form and manner in which and the Authority before whom the oath of office and of secrecy is to be subscribed by the Chairperson and Members under sub-section (2) of section 14; 10

(b) the salary and allowances payable to, and other terms and conditions of service of, the Chairperson and the allowances or remuneration payable to Members of the Authority under sub-section (5) of section 14;

(c) the other powers and functions of the Chairperson of the Authority under section 17; 15

(d) the other powers and functions of the Authority under clause (i) of sub-section (2) of section 23;

(e) the form of annual statement of accounts to be prepared by the Authority under sub-section (1) of section 26; 20

(f) the form and the manner in which and the time within which returns and statements and particulars are to be furnished under sub-section (1) of section 27;

(g) the form and the manner and the time at which the Authority shall furnish annual report under sub-section (2) of section 27;

(h) any other matter which is required to be or may be, prescribed, or in respect of which provision is to be or may be made by rules 25

Power of
Authority to
make
regulations

53. (1) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder, for carrying out the provisions of this Act

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely.— 30

(a) the biometric information under clause (e) and the demographic information under clause (h) of section 2

(b) the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (j) of section 2;

(c) the manner of furnishing the demographic information and biometric information by the resident under sub-section (1) of section 3; 35

(d) the manner of verifying the demographic information and biometric information for issue of aadhaar number under sub-section (2) of section 3;

(e) the conditions, fees and manner of authentication of the aadhaar number under sub-section (1) of section 5. 40

(f) the other functions to be performed by Central Identities Data Repository under section 7;

(g) the manner of updating biometric information and demographic information under section 8;

(h) the other categories of individuals under section 10 for whom the Authority shall take special measures for issue of aadhaar number; 45

B 11
310

(i) the time and places of meetings of the Authority and the procedure for transaction of business to be followed by it (including the quorum) under sub-section (1) of section 18,

5 (j) the salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-section (3) of section 20.

(k) the demographic information and biometric information and process for their collection and verification under clause (a) and the manner of their collection under clause (b) of sub-section (2) of section 23;

10 (l) the manner of maintaining and updating the information of individuals in the Central Identities Data Repository under clause (f) of sub-section (2) of section 23,

(m) the manner of omitting and deactivating an aadhaar number and information relating thereto under clause (g) of sub-section (2) of section 23,

15 (n) the usage and applicability of the aadhaar number for delivery of various benefits and services under clause (h) of sub-section (2) of section 23;

(o) the terms and conditions for appointment of Registrars, enrolling agencies and other service providers and the revocation of appointments thereof under clause (i) of sub-section (2) of section 23,

20 (p) the manner of sharing information of aadhaar number holder under clause (k) of sub-section (2) of section 23,

(q) various processes relating to data management, security protocol and other technology safeguards under clause (m) of sub-section (2) of section 23,

(r) the procedure for issuance of new aadhaar number to existing aadhaar number holder under clause (n) of sub-section (2) of section 23;

25 (s) manner of authorising Registrars, enrolling agencies or other services providers to collect such fees for services provided by them under clause (o) of sub-section (2) of section 23,

(t) policies and practices to be followed by the Registrar, enrolling agencies and other service providers under clause (r) of sub-section (2) of section 23;

30 (u) the allowances or remuneration and terms and conditions of consultants, advisors and other persons under sub-section (4) of section 23;

(v) the manner in which an aadhaar number holder can access his identity information under sub-section (3) of section 30,

35 (w) the manner of alteration of demographic information under sub-section (1) and biometric information under sub-section (2) of section 31;

(x) the manner of and the time for maintaining the details of request for authentication and the response thereon under sub-section (1) of section 32;

40 (y) the manner of obtaining, by the aadhaar number holder, the records of request for authentication of his aadhaar number and response thereon under sub-section (2) of section 32,

(z) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations

54. Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation, or both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation

Laying of
rules and
regulations
before
Parliament

Application of
other laws not
barred.

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

Power to
remove
difficulties.

56. (1) 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. 5

Provided that no such order shall be made under this section after the expiry of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament. 10

Savings

57. 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-Admn.L. dated the 28th January, 2009, shall be deemed to have been done or taken under the corresponding provisions of this Act.

STATEMENT OF OBJECTS AND REASONS

The Central Government had decided to issue unique identification numbers to all residents in India and to certain other persons. The scheme of unique identification involves collection of demographic information and biometric information from individuals for the purpose of issuing of unique identification numbers to such individuals. The biometric information would involve taking of a set of biological attributes of such individuals.

2. The Central Government, for the purposes of issue of the unique identification numbers, constituted, vide its notification dated the 28th January 2009 being of executive in nature, the Unique Identification Authority of India, which is at present functioning under the Planning Commission.

3. It has been observed and assessed that the issue of unique identification numbers may involve certain issues, such as (a) security and confidentiality of information, imposition of obligation of disclosure of information so collected in certain cases; (b) impersonation by certain individuals at the time of enrolment for issue of unique identification numbers; (c) unauthorised access to the Central Identities Data Repository; (d) manipulation of biometric information; (e) investigation of certain acts constituting offence; and (f) unauthorised disclosure of the information collected for the purposes of issue of the unique identification numbers which should be addressed by law and attract penalties.

4. In view of the foregoing paragraph, it has been felt necessary to make the said Authority as a statutory authority for carrying out the functions of issuing identification numbers to the residents in India in an effective manner. It is, therefore, proposed to enact the National Identification Authority of India Bill, 2010 to provide for the establishment of the National Identification Authority of India for the purpose of issuing identification numbers (which has been referred to as aadhaar number) 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 and for matters connected therewith or incidental thereto.

5. The National Identification Authority of India Bill, 2010, *inter alia*, seeks to provide—

(a) for issue of aadhaar numbers to every resident by the Authority on providing his demographic information and biometric information to it in such manner as may be specified by regulations;

(b) for authentication of the aadhaar number of an aadhaar number holder in relation to his biometric information and demographic information subject to such conditions and on payment of such fees as may be specified by regulations;

(c) for establishment of the National Identification Authority of India consisting of a Chairperson and two part-time Members;

(d) that the Authority to exercise powers and discharge functions which *inter alia*, include—

(i) specifying the demographic information and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof;

(ii) collecting demographic information and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations;

(iii) appointing of one or more entities to operate the Central Identities Data Repository;

(iv) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(v) specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations;

(e) that the Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health;

(f) that the Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations;

(g) for constitution of the Identity Review Committee consisting of three members (one of whom shall be the chairperson) to ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government;

(h) 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 unauthorised access or use or unauthorised disclosure thereof;

(i) for offences and penalties for contravention of the provisions of the proposed legislation

6. The notes on clauses explain in detail the various provisions contained in the Bill.

7. The Bill seeks to achieve the above objectives.

New Delhi;

MAN MOHAN SINGH

The 8th November, 2010.

315
814

Notes on clauses

Clause 2 — This clause contains definitions of certain words and expressions used in the proposed legislation. These definitions, *inter alia*, include the definitions of "aadhaar number", "authentication", "Central Identities Data Repository", "demographic information", "identity information", "resident", "Review Committee", etc.

Clause 3 — This clause provides for entitlement to obtain an aadhaar number by every resident. It proposes that every resident shall be entitled to obtain an aadhaar number after providing his demographic information and biometric information to the Authority in such manner as specified by regulations. It further provides that the Central Government may from time to time notify the other category of individuals who may be entitled to obtain an aadhaar number. It also provides that the Authority after verifying the demographic information and biometric information provided by the resident, issue an aadhaar number to such resident.

Clause 4 — This clause deals with the properties of aadhaar number. It provides that any aadhaar number issued to an individual shall not be re-assigned to any other individual; it shall be a random number and bear no attributes or identity data relating to the aadhaar number holder. It further provides that the aadhaar number can be accepted as proof of identity of its holder but subject to authentication.

Clause 5 — This clause empowers the Authority to perform authentication of the aadhaar number of a aadhaar 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 specified by regulations. It further empowers the Authority to respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic information and biometric information.

Clause 6 — This clause lays down that the aadhaar number or the authentication thereof shall not, by itself, confer any right of or be proof of citizenship or domicile in respect of an aadhaar number holder.

Clause 7 — This clause empowers the Authority to engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as provided under regulations.

Clause 8 — This clause deals with the updating of the demographic information and biometric information of the aadhaar number holders, from time to time, in such manner as specified by regulations so as to ensure continued accuracy of their information in the Central Identities Data Repository.

Clause 9 — This clause prohibits the Authority from requiring any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health.

Clause 10 — This clause empowers the Authority to take special measures to issue aadhaar number to women, children, senior citizens, persons with disability, migrant unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals which are specified by regulations.

Clause 11 — This clause provides for establishment of the National Identification Authority of India, by the Central Government, to exercise the powers conferred on it and to perform the functions assigned to it under the proposed legislation. The said Authority shall be a body corporate, having perpetual succession and a common seal, with power, subject to the provisions of the proposed legislation, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued. It further provides for the location of the head office of the Authority in the National Capital Region and with the prior approval of the Central Government, to establish its offices at other places in India.

Clause 12 — This clause lays down the composition of the Authority consisting of a Chairperson and two part-time Members to be appointed by the Central Government.

Clause 13.—This clause provides for qualifications for appointment of Chairperson and Members of the Authority. It provides that persons of ability, integrity and outstanding calibre having experience and knowledge in the matters relating to technology, governance, law, development, economics, finance, management, public affairs or administration shall be qualified as Chairperson and Members of the Authority.

Clause 14 — This clause provides for term of office and other conditions of service of Chairperson and Members. It provides that the Chairperson and the Members shall hold office for a term of three years from the date on which they assume office and shall be eligible for reappointment. It also provides that the Chairperson or Member of the Authority shall not hold office as such after he has attained the age of sixty-five years.

It also provides that the Chairperson of the Unique Identification Authority of India appointed before the commencement of the proposed legislation by notification A-43011/02/2009-Admin.1 (Vol.11) dated the 2nd July, 2009 shall continue as a Chairperson of the Authority under the proposed legislation for the term for which he had been appointed.

It also provides that the Chairperson and every Member shall, before entering upon their office, make and subscribe to, an oath of office and of secrecy, in such form and in such manner and before such Authority as may be prescribed.

It also provides that notwithstanding anything contained in sub-clause (1), the Chairperson or Member may relinquish his office, by giving in writing to the Central Government, a notice of not less than thirty days or be removed from his office in accordance with the provisions of clause 15. It also provides that the Chairperson shall not hold any other office during the period of holding their office in the Authority as such.

It also provides that the salaries and allowances payable to, and the other terms and conditions of service of, the Chairperson and allowances or remuneration payable to part-time Members shall be such as may be prescribed by the Central Government but neither the salary, allowances nor the other terms and conditions of service of the Chairperson shall be varied to his disadvantages after his appointment.

Clause 15.— This clause provides for removal of Chairperson and Members of the Authority. It provides that the Central Government may remove from office the Chairperson or a Member of the Authority on any of the grounds enumerated in this clause.

It further provides that the Chairperson or a Member shall not be removed from his office on the grounds specified in item (d) or (e) of sub-clause (1) unless he has been given a reasonable opportunity of being heard in respect of those charges.

Clause 16.— This clause prohibition as to holding of offices by the Chairperson or a Member on ceasing to be such Chairperson or a Member of the Authority. It provides that on ceasing to hold office, the Chairperson or Member of the Authority, as the case may be, shall subject to the provisions of the proposed legislation, be ineligible, for further 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. It also provides that the clause shall not apply to any employment under the Central Government or a State Government or local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in section 617 of the Companies Act, 1956.

It also provides prohibition to act, for or on behalf of any person or organisation in connection with any specific proceeding or transaction or negotiation or a case to which the Authority is a party and with respect to which the Chairperson or such Member had, before cessation of office, acted for or provided advice to, the Authority; to give advice to any person using information which was obtained in his capacity as the Chairperson or a Member and being unavailable to or not being able to be made available to the public; to enter, for a period of three years from his last day in office, into a contract of service with, accept an appointment to a board of directors of, or accept an offer of employment with, an entity with which he had direct and significant official dealings during his term of office as such.

317
316

Clause 17 — This clause lays down the functions of the Chairperson. It provides that the Chairperson shall have powers of general superintendence, direction in the conduct of the affairs of the Authority in addition to presiding over the meetings of the Authority and without prejudice to any of the provisions of the proposed legislation, to exercise and discharge such powers and functions of the Authority as may be prescribed.

Clause 18 — This clause empowers the Authority to determine the procedure for the transaction of business in its meetings including times and places of such meetings. It provides that the Chairperson, or, if for any reason, he is unable to attend a meeting of the Authority, the senior most Member shall preside over the meetings of the Authority.

It further provides that all questions which come up before any meeting of the Authority shall be decided by a majority of votes by the Members present and voting and in case of an equality of votes, the Chairperson or in his absence the Member presiding over shall have a second or casting vote and all such decisions of the Authority shall be authenticated by the signature of the Chairperson or any other Member authorised by the Authority in this behalf.

It also provides that any Member, who is a director of a company and who as such director, has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority he shall, as soon as possible after relevant circumstances have come to his knowledge, disclose the nature of his interest at such meeting and such disclosure shall be recorded in the proceedings of the Authority, and the Member shall not take part in any deliberation or decision of the Authority with respect to that matter.

Clause 19 — This clause enumerates the circumstances under which the acts or proceedings of the Authority shall not be invalidated. It provides that no act or proceeding of the Authority shall be invalid merely by reason of, any vacancy in, or any defect in the constitution of, the Authority, any defect in the appointment of a person as a Member of the Authority, or any irregularity in the procedure of the Authority not affecting the merits of the case.

Clause 20 — This clause makes provision for appointment of officers and other employees of Authority. It provides for the appointment of a chief executive officer of the Authority by the Central Government, who shall act as the Member-Secretary of the Authority. It also provides for determining the number, nature and categories of other officers and employees required to the Authority in the discharge of its functions.

It also provides for the determination of the salaries and allowances and the other terms and conditions of service of the chief executive officer and other officers and other employees of the Authority by regulation with the approval of the Central Government.

Clause 21 — This clause lays down functions of the chief executive officer. The functions of the chief executive officer, who shall be the legal representative of the Authority *inter alia*, shall be the day-to-day administration and implementing the work programmes and decisions adopted by the Authority; drawing up of proposal for the Authority's work programmes, the preparation of the statement of revenue and expenditure and the execution of the budget of the Authority, submitting every year a general report covering all the activities of the Authority in the previous year and programmes of work; and the annual accounts for the previous year and the budget for the coming year.

It further lays down that the chief executive officer shall have administrative control over the officers and other employees of the Authority.

Clause 22 — This clause makes provision for transfer of assets, liabilities of the Authority. It provides 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 to be established under the proposed legislation.

318
317

It further provides that all data and information collected during enrolment, all details of authentication performed, debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for such Unique Identification Authority of India for or in connection with the purpose of the said Unique Identification Authority of India, shall be deemed to have been incurred, entered into or engaged to be done by, with or for, the Authority and all sums of money due shall be deemed to be due to the Authority and all suits and other legal proceedings instituted or which could have been instituted by or against such Unique Identification Authority of India may be continued or may be instituted by or against the Authority.

Clause 23.—This clause lays down the powers and functions of Authority. It provides that the Authority shall develop the policy, procedure and systems for issuing aadhaar numbers to residents and perform authentication thereof under this Act. It further specifies the powers and functions of the Authority which, *inter alia*, include, specifying, by regulation, demographic information and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof; collecting demographic information and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations; appointing of one or more entities to operate the Central Identities Data Repository; generating and assigning aadhaar numbers to individuals; performing authentication of the aadhaar numbers; maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations; specifying the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations; specifying, by regulation, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof; establishing, operating and maintaining of the Central Identities Data Repository; calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of the proposed legislation of the Central Identities Data Repository; Registrars, enrolling agencies and other agencies appointed under this Act; specifying, by regulation, the conditions and procedures for issuance of new aadhaar number to existing aadhaar number holder, levy and collect the fees or authorise the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under the proposed legislation in such manner as may be specified by regulations.

It also empowers the Authority to enter into a Memorandum of Understanding or agreement, as the case may be, with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or performing authentication; and appoint by notification, such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto, as may be necessary for the purposes of the proposed legislation or to engage such consultants, advisors and other persons as may be required for efficient discharge of its functions under this Act on such allowances or remuneration and terms and conditions as may be specified by regulations.

Clause 24.—This clause makes provision for grants by the Central Government. It provides that after due appropriation made by Parliament by law the Central Government may make grants of such sums of money as it may think fit to the Authority for being utilised for the purposes of the proposed legislation.

Clause 25.—This clause provides for other fees and revenue. It provides that fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India and entire amount so credited shall be transferred to the Authority.

Clause 26.—This clause makes provision for accounts and audit. It provides that the Authority shall maintain proper accounts and other relevant records and prepare an annual statement of account, in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

819
318

It further provides that the accounts of the Authority shall be audited annually by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Authority to the Comptroller and Auditor-General.

It also provides that the accounts of the Authority, as certified by the Comptroller and Auditor-General or any other person appointed by him in this behalf together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the audit report to be laid, as soon as may be after it is received, before each House of Parliament.

Clause 27.—This clause provides for returns and annual report, etc. It provides that the Authority shall furnish to the Central Government at such time and in such form and 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.

It further provides that the Authority shall prepare, once in every year, and in such form and manner and at such time as may be prescribed, an annual report giving a description of all the activities of the Authority for the previous years, the annual accounts for the previous year, and the programmes of work for coming year. A copy of such report shall be laid by the Central Government before each House of Parliament.

Clause 28 — This clause provides for the Review Committee. It provides that the Central Government may, by notification, constitute the Identity Review Committee, consisting of three members (one of whom shall be the chairperson as such designated by the Central Government) who are persons of eminence, ability, integrity and standing in public life having knowledge and experience in the fields of technology, law, administration and governance, social service, journalism, management or social sciences, to discharge functions specified under sub-clause (1) of clause 29 in respect of any matter connected with the usage of the aadhaar numbers.

It further provides that the members of the Review Committee shall be appointed by the Central Government on the recommendations of a committee consisting of the Prime Minister, who shall be the chairperson of the committee; the Leader of Opposition in the Lok Sabha; and a Union Cabinet Minister to be nominated by the Prime Minister.

It also provides that the member of the Review Committee shall not be a Member of Parliament or Member of the Legislature of any State or Union territory as the case may be or a member of any political party. A member 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 and may be removed by the Central Government on the grounds specified under sub-clause (6).

Clause 29 — This clause makes provision for functions of the Review Committee. It provides that the Review Committee shall ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government. This clause further empowers the Review Committee to determine the manner of preparation of the report. It also provides that a 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.

Clause 30.—This clause provides for security and confidentiality of information. It provides that the Authority shall ensure the security and confidentiality of identity information and authentication records of individuals and 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 unauthorised access or use or unauthorised disclosure thereto.

It further provides that notwithstanding anything contained in any other law for the time being in force and save as otherwise provided in the proposed legislation, the Authority or any of its officer or other employee or any agency who maintains the Central Identities Data Repository shall not reveal any information stored in the Central Identities Data Repository to any person but an aadhaar number holder may request the Authority to provide access to his identity information in such manner as may be specified by regulations.

Clause 31.—This clause makes provision relating to alteration of demographic information or biometric information. It provides that in case any demographic information relating to an aadhaar number holder is found incorrect or it changes subsequently, and in case any biometric information of aadhaar number holder is lost or changes subsequently for any reason, then the aadhaar number holder shall request the Authority to alter such demographic information or biometric information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

It further provides that on receipt of any request for alteration of demographic information or biometric information, the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such aadhaar number holder and intimate such alteration to the concerned aadhaar number holder.

Clause 32.—This clause makes provision for access to own information and records of requests for authentication. It provides that the Authority shall maintain details of every request for authentication of the identity of every aadhaar number holder and the response provided thereon by it in such manner and for such time as may be specified by regulations. It further provides that every aadhaar number holder shall be entitled to obtain details of request for authentication of his aadhaar number and the response provided thereon by the Authority in such manner as may be specified by regulations.

Clause 33.—This clause provides for disclosure of information in certain cases. It provides that provisions of sub-clause (3) of clause 30 which impose restrictions on providing information shall not apply in respect of any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorised in this behalf by an order of the Central Government.

Clause 34.—This clause provides for penalty for impersonation at time of enrolment. It provides that whoever impersonates or attempts 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.

Clause 35.—This clause provides for penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information. It provides that whoever, with the intention of causing harm or mischief to a aadhaar number holder, or with the intention of appropriating the identity of a aadhaar number holder changes or attempts to change any demographic information or biometric information of a aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, 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.

Clause 36.—This clause provides for penalty for impersonation. It provides that whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorised 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.

Clause 37.—This clause provides for penalty for disclosing identity information. It provides that whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised 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.

Clause 38.— This clause provides for penalty for unauthorised access to the Central Identities Data Repository. It provides that whoever, not being authorised by the Authority, intentionally, (a) accesses or secures access to the Central Identities Data Repository or (b) downloads, copies or extracts any data from the Central Identities Data Repository; or stored in any removable medium or (c) introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository; or (d) damages or causes to be damaged the data in the Central Identities Data Repository; or (e) disrupts or causes disruption of the access to the Central Identities Data Repository; or (f) denies or causes a denial of access to any person who is authorised to access the Central Identities Data Repository; or (g) provides any assistance to any person to do any of the acts aforementioned, (h) destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or effects it injuriously by any means, (i) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage, shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which shall not be less than one crore rupees.

It further defines the expressions 'computer contaminant', 'computer virus' and 'damage' to have the same meanings for the purposes of this clause as are respectively assigned to them in the *Explanation* to section 43 of the Information Technology Act, 2000.

Clause 39 — This clause provides for penalty for tampering with data in Central Identities Data Repository. It provides that whoever, not being authorised by the Authority, uses or tampers with the data in the Central Identities Data Repository or in any removable storage medium with the intent of modifying information relating to aadhaar 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.

Clause 40.— This clause provides for penalty for manipulating biometric information. It provides that whoever gives or attempts to give any biometric information which does not pertain to him for the purpose of getting an aadhaar number or authentication or updating his information, 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 with both.

Clause 41.— This clause provides for general penalty. It provides that whoever, commits an offence under the proposed legislation for which no penalty is provided elsewhere than in this clause, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Clause 42.— This clause deals with the offences by companies. It provides that where an offence under the proposed legislation has been committed by a company then every person who at the time when the alleged 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.

It further provides that if any such person proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence, then he shall not be liable for the said punishment.

It also provides that where any offence under the proposed legislation 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.

Clause 43.— This clause makes provision for application of the proposed legislation in relation to offence or contravention committed outside India. It provides that the provisions of the proposed legislation shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves the Central Identities Data Repository.

Clause 44 — This clause provides for power to investigate offences. It provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector of Police shall investigate any offence under the proposed legislation.

Clause 45.— This clause relates to penalties not to interfere with other punishments. It provides that no penalty imposed under the proposed legislation shall prevent the imposition of any other penalty or punishment under any other law for the time being in force.

Clause 46.— This clause provides for cognizance of offences. It provides that any court shall not take cognizance of any offence punishable under the proposed legislation, save on a complaint made by the Authority or any officer or person authorised by it.

It further provides that any court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall not try any offence punishable under the proposed legislation.

Clause 47 — This clause empowers the Central Government to supersede Authority. It provides that the Central Government may after satisfying on the ground mentioned under this clause supersede the Authority by issuing a notification for such period not exceeding six months and appoint a person or persons as the President may direct to exercise powers and discharge functions under the proposed legislation.

It further provides 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.

It also provides that upon the publication of a notification superseding the Authority, (a) the Chairperson and other members shall, as from the date of supersession, vacate their offices as such, (b) all the powers, functions and duties which may, by or under the provisions of this Act, be exercised or discharged by or on behalf of the Authority shall, until the Authority is reconstituted, be exercised and discharged by the person or persons referred to in sub-clause (1); and (c) all properties owned or controlled by the Authority shall, until the Authority is reconstituted under sub-section (3), vest in the Central Government.

It also provides that the Central Government shall reconstitute the Authority, before the expiration of the period of supersession, by a fresh appointment of its Chairperson and other members and in such case any person who had vacated his office due to supersession of the Authority shall not be deemed to be disqualified for reappointment.

It also provides that the Central Government shall cause a copy of the notification and a full report of any action taken under this clause and the circumstances leading to such action to be laid before each House of Parliament at the earliest.

Clause 48.— This clause provides that Members, officers, etc., to be public servants. It provides 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 the proposed legislation, to be public servants within the meaning of section 21 of the Indian Penal Code.

Clause 49.—This clause empowers the Central Government to issue directions. It provides that without prejudice to the foregoing provisions of the proposed legislation, the Authority shall, in exercise of its powers or the performance of its functions, 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.

It further provides that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this clause. It also provides that the decision of the Central Government, whether a question is one of policy or not, shall be final.

Clause 50.—This clause provides for delegation. It provides that the Authority may, by general or special order in writing, delegate to any Member, officer of the Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under clause 53 relating to making of regulations) as it may deem necessary.

Clause 51.—This clause provides for protection of action taken in good faith. It provides that any suit, prosecution or other legal proceeding shall not 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 the proposed legislation or the rules or regulations made thereunder.

Clause 52.—This clause empowers the Central Government to make rules. It provides that the Central Government may, by notification, make rules to carry out the provisions of the proposed legislation. It further specifies the matters in respect of which such rules may be made.

Clause 53.—This clause empowers the Authority to make regulations. It provides that the Authority may, by notification, make regulations for carrying out the provisions of the proposed legislation consistent with the proposed legislation and the rules made thereunder. It further specifies the matters in respect of which such regulations may be made.

Clause 54.—This clause provides for laying of rules and regulations before Parliament. It provides that every rule and every regulation made under the proposed legislation shall be laid, as soon as may be after it is made, before each House of Parliament.

Clause 55.—This clause provides that the provisions of the proposed legislation shall be in addition to, and not in derogation of, any other law for the time being in force.

Clause 56.—This clause makes provision for removal of difficulties. It provides that if any difficulty arises in giving effect to the provisions of the proposed legislation then the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of the proposed legislation as may appear to be necessary for removing the difficulty.

It further provides that any such order for removal of difficulty shall be made under this section within a period of two years from the commencement of the proposed legislation.

It also provides that every order made under this clause shall be laid, as soon as may be after it is made, before each House of Parliament.

Clause 57.—This clause provides for savings. It provides that 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 the proposed legislation.

324
323

FINANCIAL MEMORANDUM

Clause 11 provides for establishment of the National Identification Authority of India which shall be a body corporate having perpetual succession and a common seal with power to acquire, hold and dispose of property and sue or be sued with the head office in the National Capital Region and may establish its offices at other places in India. Clause 12 provides that Authority shall consist of a Chairperson and two part-time Members. Sub-clause (5) of clause 14 makes provision for salaries and allowances payable to the Chairperson and allowances or remuneration payable to part-time Members. Sub-clause (3) of clause 20 makes provision for salaries and allowances payable to the chief executive officer and other officers and other employees of the Authority.

2. Item (j) of sub-clause (2) of clause 23 provides for establishment, operation and maintenance of the Central Identity Data Repository.

3. Clause 24 provides 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 utilised for the purposes of the proposed legislation.

4. Clause 25 of the Bill provides that the fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India and the entire amount so credited will be transferred to the Authority.

5. It is estimated that there would be an expenditure of approximately Rs. 3023.01 crore in phase two of the scheme. Out of this, an amount of Rs. 477.11 crore would be towards recurring establishment expenditure and Rs. 2,545.90 crore would be towards non-recurring project related expenditure. The estimated cost for the first phase of the scheme was Rs. 147.31 crore towards the setting up necessary infrastructure for offices at headquarters and regional headquarters, creating testing facilities for running the pilots and proof of concept studies, initial work of creating standards in various areas of operations, and setting up of a project management unit and hiring of consultants.

6. The Bill does not envisage any other expenditure of recurring or non-recurring nature.

324
325

MEMORANDUM REGARDING DELEGATED LEGISLATION

Sub-clause (1) of clause 52 of the Bill empowers the Central Government to make, by notification, rules to carry out the provisions of the proposed legislation. Sub-clause (2) specifies the matters in respect of which such rules may be made. These matters, *inter alia*, include: (a) the form and manner in which and the authority before whom the oath of office and of secrecy is to be subscribed by the Chairperson and Members under sub-clause (2) of clause 14; (b) the salary and allowances payable to, and other terms and conditions of service of, the Chairperson and the allowances or remuneration payable to Members of the Authority under sub-clause (5) of clause 14; (c) the other powers and functions of the Chairperson of the Authority under clause 17; (d) the other powers and functions of the Authority under item (i) of sub-clause (2) of clause 23; (e) the form of annual statement of accounts to be prepared by Authority under sub-clause (1) of clause 26; (f) the form and the manner in which and the time within which returns and statements and particulars are to be furnished under sub-clause (1) of clause 27; (g) the form and the manner and the time at which the Authority shall furnish annual report under sub-clause (2) of clause 27; (h) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be or may be made by rules.

2. Sub-clause (1) of clause 53 of the Bill empowers the National Identification Authority of India to make, by notification, regulations to carry out the provisions of the proposed legislation consistent with the provisions of the proposed legislation and the rules made thereunder. Sub-clause (2) specifies the matters in respect of which such regulations may be made. These matters, *inter alia*, include: (i) the biometric information under sub-clause (e); the demographic information under sub-clause (h); the process of collecting demographic information and biometric information from the individuals by enrolling agencies under sub-clause (j) of clause 2; (ii) the manner of furnishing the demographic information and biometric information by the resident under sub-clause (1) of clause 3; and the manner of verifying the demographic information and biometric information for issue of aadhaar number under sub-clause (2) of clause 3; (iii) the procedure for authentication of the aadhaar number under sub-clause (1) of clause 5; (iv) the other functions to be performed by Central Identities Data Repository under clause 7; (v) the manner of updating biometric information and demographic information under clause 8; (vi) the other categories of individuals under clause 10 for whom the Authority shall take special measures for allotment of aadhaar number; (vii) the time and places of meetings of the Authority and the procedure for transaction of business to be followed by it (including the quorum) under sub-clause (1) of clause 18; (viii) the salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-clause (3) of clause 20; (ix) various matters specified under clause 23; (x) the manner of accessing the identity information by the aadhaar number holder under sub-clause (2) of clause 30; (xi) the manner of alteration of demographic information under sub-clause (1) and biometric information under sub-clause (2) of clause 31; (xii) the manner of and the time for maintaining the request for authentication and the response thereon under sub-section (1) and the manner of obtaining, by the aadhaar number holder, the records of request for authentication and response thereon under sub-clause (2) of clause 32; (xiii) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations.

3. Clause 54 provides that every rule and every regulation made under the proposed legislation shall be laid, as soon as may be after it is made, before each House of Parliament.

4. The matters in respect of which rules and regulations may be made are matter of procedure or administrative detail and it is not practicable to provide for them in the Bill itself. The delegation of legislative power is therefore of a normal character.

325 326

RAJYASABHA

A

FRLL

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 and for matter connected therewith or incidental thereto.

(Shri V. Narayanasamy, Minister of State in the Ministry of Planning and Parliamentary Affairs)

GMGIPMRND—514/RS—11.11.2010

True copy
P
Adv

A Unique Identity Bill

USHA RAMANATHAN

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. As has been observed, the Constitution is expected to provide the citizen with dignity and privacy; but these are missing in the UID project.

Thanks to Pavithra Ramesh and Murali for acting as sounding boards

Usha Ramanathan (uramanathan@rediffmail.com) is an independent law researcher who works on the jurisprudence of law, poverty and rights

In February 2009, the unique identification number (UID) project was set up within the Planning Commission. Since August (July) 2009, when Nandan Nilekani was appointed as its chairperson, the Unique Identification Authority of India (UIDAI) has been propagating the idea of the UID which each resident in India will be given.

The project pegs its legitimacy on what it will do for the poor. It promises that it will give the poor an identity, with which they may become visible to the state. The UID number is expected to plug leakages, including in the 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 entitlements"

The UID database is intended to hold information including the name, address 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 UIDAI has strained every nerve to explain that it will not be a database from which others may derive information about any person. The UIDAI will merely "authenticate", i.e., it will give a "yes" or "no" answer when asked whether a name, address and biometric indicator tally. That is, it will attest to the veracity of the identity being asserted by a person by checking on its database. If the details tally, it will say no more.

The operation for being invested with an identity goes through stages: enrolling with an enrollee/registrar who will set down the basic biographic details such as

name, address, father/guardian's name (and UID number), mother's name (and UID number) and collect the biometrics – photographs, all 10 fingerprints and iris scan, de-duplication (which will be done by the UIDAI to make certain that there is one identity for one person), updating the database whenever any change occurs in relation to the information on the database (for instance, when there is a name or address change, the responsibility for which will rest with the individual)

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, if other agencies make the UID number essential in their transactions, that is a different matter. The UIDAI has been signing memoranda of understanding (MOUs) with a range of agencies including banks, state governments and the Life Insurance Corporation of India (LIC) to be "registrars", who then may insist that their customers enrol on the UID to receive continued service.

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 salience 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.

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 routinised in recent years has eroded the relevance of traditional notions of privacy. The experience with abandoning the idea of privacy is relatively recent, and it will be a while before its value is reconstituted and the idea resurrected. The introduction to the UID has been in terms of investing every resident

with an identity, as a single stop for authenticating 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. They include the contexts of convergence, national security, the national population register (NPR), and the shaky edifice of biometrics on which this superstructure is being built.

Convergence

The urn literature does not use the word, yet convergence is a predictable and inevitable consequence of the urn project. Convergence is about combining information. There are various pieces of information that we hand over to a range of agencies when buying, say, a railway ticket, maintaining a bank account, registering in a university, getting work at an NRGS worksite, taking out an insurance policy, buying a motorcycle, paying telephone bills, etc. Currently, with only the name and a possibly correct address, it will not be easy to profile a person or track them. The information is held in what are called "silos", that is, discrete towers holding information that has been handed over by an individual in relation to a defined purpose. If it were possible to create bridges to link these silos, it would wrest control of information on the individual and make it available, metaphorically and literally, at the tap of a computer key.

There is a dark joke making its rounds which would be funny, but is not, and it runs like this

Operator: Thank you for calling Pizza Plaza. May I have your ..

Customer: May I place an order?

Operator: Can I have your multipurpose ID card number, sir?

Customer: It is, hold on ... 21356102049998-45-54610

Operator: Welcome back from Japan, Mr Singh

Customer: May I order your Seafood Pizza

Operator: That's not a good idea, sir

Customer: Why would you say that?

Operator: According to your medical records, sir, you have high blood pressure and even higher cholesterol level.

Customer: What? .. What do you recommend then?

Operator: Try our Low Fat Pizza. You'll like it

Customer: How would you know that?

Operator: You borrowed a book titled *Popular Dishes* from the National Library last week, sir

Customer: Oh .. Have three family size delivered. How much would that cost?

Operator: That should be enough for your family of 5, sir. That will be Rs 500.

Customer: Do you accept payment by credit card?

Operator: I'm afraid you have to pay us cash, sir. Your credit card is over the limit and you owe your bank Rs 23,000 since October last year. And that's not including the late payment charges on your housing loan.

Customer: I guess I have to run to the neighbourhood ATM and withdraw some cash before you gawk at us.

Operator: Oh, no, sir. Your records show that you've reached your daily limit on machine withdrawal today.

Customer: Never mind, just send the pizzas, I'll have the cash ready. How long will that take?

Operator: About 45 minutes, sir, but if you can't wait you can always come and collect it in your Nano. Will there be anything else, sir?

Customer: No. By the way, make sure you send the 3 litre bottle of cola as advertised.

Operator: But, sir, your health records say you're a diabetic. ..

Customer: #\$\$^%&\$@%\$% ^

Operator: Please watch your language, sir. Remember on 15 July you were convicted of using abusive language at a policeman?

It was reported last year that Apollo Hospitals had written to the UIDAI and to the Knowledge Commission to link urn numbers with health profiles of individuals and offered to manage the health records (*Business Standard*, 27 August 2009). It has already embarked on a project "Health Superhighway" that reportedly connects doctors, hospitals and pharmacies, who would be able to communicate with each other and access health records. This, then, is no longer hypothetical. The urn is poised to be the bridge between silos of personal information.

This convergence of information may be efficient for business and meet standards of efficiency, but there are those who would argue that it profiles individuals and exposes them to market and other forces in ways which are intrusive, and which could make them insecure, and unsafe.

National Security

Surveillance is a concern, and a term that is missing altogether in the UIDAI documents.

There are three initiatives that together, form a pattern that is disturbing. The urn 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 Jesited information for intelligence and enforcement agencies" (*The Hindu*, 14 February 2010). "This is to enable them to detect patterns, trace sources for monies and support, track travellers, and identify those who must be watched, investigated, disabled and neutralised". Many of these intelligence agencies, including the Research and Analysis Wing (RAW) and the Intelligence Bureau (IB), are neither creatures of the law, nor are they subject to oversight. And they are outside the Right to Information Act. Vice-President Hamid Ansari, quoting an intelligence expert, reportedly asked, "How shall a democracy ensure its secret intelligence apparatus becomes neither a vehicle for conspiracy nor a suppressor of traditional liberties of democratic self-government?" (*Times of India*, 20 January 2010). By all accounts, the question has not been answered yet.

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 use of science and technology to practise the politics of suspicion is a possibility that is finding its way into becoming a fact.

National Population Register

The Census has acquired a disturbing dimension with the NPR being appended to it. The NPR is not an exercise undertaken under the Census Act, 1948. It is being

COMMENTARY

carried out under the Citizenship Act of 1955 and the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003. Why should that matter? Because there is an express provision regarding "confidentiality" in the Census Act, which is not merely missing in the Citizenship Act and Rules. But there is an express objective of making the information available to the UIDAI, which marks an important distinction between the two processes. Section 15 of the Census Act categorically makes the information that we give to the census agency "not open to inspection nor admissible in evidence". The Census Act enables the collection of information, so the state has a profile of the population; it is expressly not to profile the individual.

It is the admitted position that the information gathered in the house-to-house survey, and the biometrics collected during the exercise, will feed into the UID database. The UID document says the information that the database will hold will only serve to identify if the person is who the person says he, or she, is. It will not hold any personal details about anybody. What the document does not say is that it will provide the bridge between the "silos" of data that are already in existence, and which the NPK will also bring into being. So, with the UID as the key, the profile of any person resident in India can be built up.

The Citizenship Rules 2003 strips the veneer of voluntariness from the UID. It classes every individual and every "head of family" as an informant, who will be penalised if every person in the household is not in the NPK, or if the information is outdated.

The NPK is also slated to collect biometrics — photographs, fingerprints, iris. The coercion in the Citizenship Rules is not the only aspect which is worrying. The rules also envisage an exercise in sifting the citizen from the resident. The person collecting the information is expected to exercise judgment in deciding whether the person whose details are being taken down may not be a citizen. If there is any doubt, such person will be categorised to be subject to further investigation. The NPK, like the Census, is carried out by lay-people, and the untrained mind is asked

to discern and judge matters that could lead to inclusion, or statelessness.

At the tail end of June 2010, the UIDAI web site uploaded a "proposed draft bill": the National Identification Authority of India Bill, 2010. Comments were asked to be sent within two weeks, by 13 July 2010. Various individuals and groups have sent in their comments, but have asked that the time to respond be extended so that they may discuss it and understand it more fully before taking their position on the Bill.

One of the provisions that has raised concern is clause 31, which reads:

31. Nothing contained in the sub-section (2) of section 30 shall apply in respect of—

- (a) any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or
- (b) any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer not below the rank of Joint Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge.

Although some commentators on the UID project (and that includes me) have written about surveillance, tracking, profiling and social and executive control of the people by the state and its agents, the UIDAI has not acknowledged these concerns so far. This is despite the "Awareness and Communication Report" which the

UIDAI commissioned and which advised the authority on how to anticipate and sidestep the unease that people may have, registering that:

the idea of giving out information and affixing one's thumbprint to a document without fully understanding its implications, compounded with the fact that too many non-state players are visibly involved could pose a barrier to enrolment as well. The fear of individuals being in the government's radar and the ability of various groups to play on this fear is another likely challenge.

Neither the Bill nor any document produced in the process has, however, addressed any of these concerns. What is reflected in the document is only the need to ensure that these anxieties do not come in the way of completing the exercise.

Such a major shift in public policy surely cannot occur without a discussion preceding it, a deliberation on the import, and consequences, of such a change, and a reasoned decision taken on the matter. The constitutionality of such a move is questionable. Among the issues that are likely to arise, there are two that Justice Rajendra Babu raised in the presence of Nandan Nilekani and his team at a consultation held in the National Law School, Bangalore on 23 November 2009: the Constitution guarantees us dignity and privacy, he said. Both seem to have been given a miss in the way the UID project has been conceived.



M.Phil in Development Studies



Admission for Fifth Batch (2010-12)

Institute of Development Studies Kolkata in collaboration with the Centre for Social Sciences and Humanities, Calcutta University, invites applications for admission to M.Phil in Development Studies (Degree to be conferred by University of Calcutta) commencing in October 2010. The two-year full-time multidisciplinary programme is offered to those who wish to pursue a career in academia, administration, NGOs, media and related fields. Candidates awaiting for PG Part II results may also apply.

For eligibility, course fee and other information please visit our website: www.idsk.edu.in.

Last date of submission of application: 12 August, 2010

Amiya Kumar Bagchi, Director,
Institute of Development Studies Kolkata
Calcutta University Alipore Campus, 1 Reformatory Street,
Kolkata-700027

The combination of UID, NATGRID and the emerging idea of the DNA bank, makes state control of a population a very real possibility. To treat every person as a suspect, and to create systems that would support such a practice, is a highly questionable act of a state. That the State and its agents have faced the charge of being communal and of having been involved in torture, fake encounters, forced disappearances and complicity in crime adds to the amalgam of concerns. The Bill does not acknowledge it, but those within the system cannot be prosecuted without sanction of the powers-that-be. It seems like a prescription for impunity where the protocol for protecting the data is breached from within the state apparatus.

Discussions around the Bill will have to deal with the issues thrown up by the introduction of the element of "national security", especially as it is located within a web of UID, NATGRID and a DNA data bank.

Biometrics

The most disturbing aspect of the UID project is the linking of identity, and rights, entitlements, citizenship and recognition, to biometrics. The UID project has settled on three metrics: facial recognition through the photograph, fingerprints (all eight fingers and two thumbs), and the iris. The UIDAI documents reveal a state of ignorance, and unpreparedness, that is inexplicable. Quotes will set it out most clearly:

In the UIDAI's "Notice Inviting Application for Hiring Biometrics Consultant", for a period of six months starting March 2010, it was written:

While NIST (the United States agency) documents the fact that the accuracy of biometric matching is extremely dependent on demographics and environmental conditions, there is a lack of a sound study that documents the accuracy achievable on Indian demographics (i.e., larger percentage of rural population) and in Indian environmental conditions (i.e., extremely hot and humid climate and facilities without air-conditioning)... The 'quality' assessments of fingerprint data is not sufficient to fully understand the achievable de-duplication accuracy. The next step is to acquire biometrics data from the Indian rural conditions in two sessions (with a time difference) and assess the matchability...

That is, the capacity to capture biometrics with any accuracy *has not even been*

tested yet, and the project already has Rs 7 crore committed to it for just this year, and the whole apparatus through the NPK moving for it. This demands an explanation.

In a cryptic note, the Notice reads: "The biometric evaluations are statistical. The statistical significance of the results are required to be analysed for the UIDAI."

That is, the margin of error is not yet known.

In 'Ensuring Uniqueness: Collecting Iris Biometrics for the Unique ID Mission', the report refers to the Biometrics Committee set up under the UIDAI which had, in January 2010, been non-committal about the use of the third biometric, since "in the absence of empirical Indian data, it is not possible for the committee to precisely predict the improvement in the accuracy of de-duplication to the fusion of fingerprint and iris scores." The document acknowledges "technology risks", including the inability to guarantee biometrics of "high quality across its thousands of enrolment points". This capture would help in enrolment, but not in authentication since the equipment will not be available in most places. The compromise "for authentication, the use of fingerprinting will be sufficient". This could spell trouble for calloused hands and marred fingerprints – which would include those doing manual labour and agricultural operations, whose fingerprints cannot be authenticated.

On 17 July 2010, the *Economic Times* reported that "people with 'low-quality' fingerprints and corneal/cataract problems" could "pose difficulties" for the project. "Millions of Indians working in agriculture, construction workers and other manual labourers have worn-out fingers due to a lifetime of hard labour" resulting in "low-quality" fingerprints. The iris scan cannot be done on people with corneal blindness or corneal scars. A study done in 2005 at the All India Institute of Medical Sciences estimated six to eight million people in India had corneal blindness, and many more people would have corneal scars. A Hyderabad based eye institute identified cataract, which results from nutritional deficiency and prolonged exposure to sunlight and ultra-violet rays, and cataract surgery, as

almost certain to affect the iris. This is about the people that the UIDAI projects as its main targets. A scientist with the Council of Scientific and Industrial Research is cited as suggesting that "they could use DNA fingerprinting in such cases". Apart from the reduction of a people to a subject-population, these suggestions are inexcusably casual about using techniques that will be of no help to the person so identified.

The draft Bill does not deal with any of these concerns. In clause 3 (1), it declares that "every resident shall be entitled to obtain" a UID number, but nowhere in the Bill is there a clause that no agency may refuse services to a person because they do not have such a number, thus leaving the field open for compulsion. Nowhere in the Bill is there an acknowledgement of the extraordinary powers of surveillance, and invasion of privacy by government and private agencies that the UID will be facilitating, so there are no limits set on the uses of the number and of the networks of information it could be used to generate. So convergence is facilitated, and the person has no control over it, nor is it a wrong in law.

For those who are willing to place their faith in the UID clause 12 may cause them to pause. It reads: "The Authority shall consist of a Chairperson and two part-time members to be appointed by the Central Government", and they may be re-appointed, or ejected, by the central government. There are sketchy offences of "intentionally" accessing the UID database and damaging, stealing, altering information or disrupting the data. But it provides no means by which a person whose data is stored to know that such an offence has been committed; and it does not allow prosecution to be launched except on a complaint made by the authority or someone authorised by it. Experience has revealed the failure of regulation; yet it is on regulation by the authority that a whole population is asked to place its trust. There is no grievance redressal mechanism mandated by law; it may be set up by regulation or it may not. There is a clause in passing that recognises that the data could reach people beyond the borders; but no idea at all on how to deal with that situation.

The demographic information gathered may not be elaborate at the start,

331
830

COMMENTARY

but clause 23(b) leaves an opening for expanding the demographic and biometric data that may be collected. Most damning is the passing reference in the general "powers and functions of authority" to the use of the uid number "for delivery of various benefits and services as may be provided by regulation". That is all there is to indicate that service delivery to the poor is the object of this exercise. The issues on which the uid project is piggyback riding for its legitimacy are too serious to be trivialised.

The move the UIDAI has entered into with "registrars" that include banks, state governments and the LIC have been signed with no statutory backing and no legal power to collect, hold and transmit information from and about people. Biometrics has not even been tested, despite Indian demographic and environmental conditions being known to make a significant difference to the quality of biometric capture. In a May 2010 paper prepared for the UIDAI - "A uid Numbering Scheme" - is written: "We expect the uid system to live on for centuries". This, then, is a tagging

device that is expected to last well beyond a person's lifetime.

The non-seriousness of the Bill, and the refusal to confront the hard issues, are a slight to democracy which must be remedied before the project progresses to create a fait accompli. There are murmurs that the Bill is to be introduced in the monsoon session of Parliament. It would be trite to say that, when biometric accuracy is still in question, and so many questions remain unanswered, it is nowhere near time for parliamentary consideration, or approval.

True Copy
F
Adv

42

STANDING COMMITTEE ON FINANCE
(2011-12)

FIFTEENTH LOK SABHA

Ministry of Planning

THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA
BILL, 2010

FORTY-SECOND REPORT



LOK SABHA SECRETARIAT
NEW DELHI

December, 2011/ Agrahyana, 1933 (Saka)

333

333

FORTY-SECOND REPORT

**STANDING COMMITTEE ON FINANCE
(2011-2012)**

(FIFTEENTH LOK SABHA)

Ministry of Planning

**THE NATIONAL IDENTIFICATION AUTHORITY OF
INDIA BILL, 2010**

Presented to Lok Sabha on 13 December, 2011

Laid in Rajya Sabha on 13 December, 2011



**LOK SABHA SECRETARIAT
NEW DELHI**

December, 2011/ Agrahyana, 1933 (Saka)

CONTENTS

PAGE

| | |
|------------------------------------|-------|
| Composition of the Committee | (iii) |
|------------------------------------|-------|

| | |
|--------------------|------|
| Introduction | (iv) |
|--------------------|------|

REPORT

| | |
|---|----|
| A. Introduction | 1 |
| B. Objectives and Salient Features of the Bill | 2 |
| C. Evolution of the UIDAI | 3 |
| D. Issuance of aadhaar numbers pending passing the Bill by Parliament | 5 |
| E. UID scheme | 7 |
| F. Global Experience | 9 |
| G. Existing Identity forms vs need for aadhaar number | 10 |
| H. Identity and Eligibility | 11 |
| I. Aadhaar Number and National Population Register (NPR) | 12 |
| J. Coordination between the agencies involved in the UID scheme | 13 |
| K. Civil Liberties Perspective | 16 |
| L. Financial Implications | 17 |
| M. Technology | 20 |
| N. National Security vs the UID scheme | 21 |

Part-II

| | |
|---|----|
| Observations/Recommendations of the Committee | 28 |
|---|----|

APPENDICES

| | |
|---|----|
| i. Dissent notes submitted by S/Shri Prem Das Rai, MP, Manicka Tagore, MP and Raashid Alvi, MP..... | 36 |
| ii. Minutes of the sittings of the Committee held on 11 February, 2011, 29 June, 2011, 29 July, 2011 and 8 December, 2011.... | 39 |
| iii. The National Identification Authority of India Bill, 2010 | 49 |

335
334

COMPOSITION OF STANDING COMMITTEE ON FINANCE – 2011-2012

Shri Yashwant Sinha - Chairman

MEMBERS

LOK SABHA

2. Shri Shivkumar Udas Chanabasappa
3. Shri Jayant Chaudhary
4. Shri Harishchandra Deoram Chavan
5. Shri Bhakta Charan Das
6. Shri Gurudas Dasgupta
7. Shri Nishikant Dubey
8. Shri Chandrakant Khaire
9. Shri Bhartruhari Mantab
10. Shri Anjan Kumar Yadav M.
11. Shri Prem Das Rai
12. Dr. Kavuru Sambasiva Rao
13. Shri Rayapati S. Rao
14. Shri Magunta Sreenivasulu Reddy
15. Shri Sarvey Sathyanarayana
16. Shri G.M. Siddeswara
17. Shri N. Dharan Singh
18. Shri Yashvir Singh
19. Shri Manicka Tagore
20. Shri R. Thamaraiselvan
21. Dr. M. Thambidurai

RAJYA SABHA

22. Shri S.S. Ahluwalia
23. Shri Raashid Alvi
24. Shri Vijay Jawaharlal Darda
25. Shri Piyush Goyal
26. Shri Moinul Hassan
27. Shri Satish Chandra Misra
28. Shri Mahendra Mohan
29. Dr. Mahendra Prasad
30. Dr. K.V.P. Ramachandra Rao
31. Shri Yogendra P. Trivedi

SECRETARIAT

- | | | |
|---------------------------------|---|------------------|
| 1. Shri A.K. Singh | - | Joint Secretary |
| 2. Shri R.K. Jain | - | Director |
| 3. Shri Ramkumar Suryanarayanan | - | Deputy Secretary |

(iii)

335
336

INTRODUCTION

1. I, the Chairman of the Standing Committee on Finance, having been authorized by the Committee, present this Forty-Second Report on "The National Identification Authority of India Bill, 2010".
2. The National Identification Authority of India Bill, 2010 introduced in Rajya Sabha on 3 December, 2010 was referred to the Committee on 10 December, 2010 for examination and report thereon, by the Speaker, Lok Sabha under Rule 331E of the Rules of Procedure and Conduct of Business in Lok Sabha
3. The Committee obtained background note, detailed note and written information on various provisions contained in the aforesaid Bill from the Ministry of Planning
4. Written suggestions / views / memoranda on the provisions of the Bill were received from various institutions / experts / individuals.
5. The Committee took briefing / oral evidence of the representatives of the Ministry of Planning and the Unique Identification Authority of India (UIDAI) at their sitting held on 11 February, 2011.
6. At the sitting held on 29 June, 2011, the Committee heard the views of the representatives of (i) the National Human Rights Commission (NHRC), and (ii) the Indian Banks Association (IBA), and Dr. Reetika Khera, Visitor, Delhi School of Economics, New Delhi. The Committee also heard the views of the representatives of the Confederation of Indian Industry (CII), and experts namely, Dr. Usha Ramanathan, Independent Law Researcher, New Delhi, Dr. R. Ramakumar, Associate Professor, the Tata Institute of Social Sciences, Mumbai and Shri Gopal Krishna, Member, Citizen Forum for Liberties, New Delhi at the sitting held on 29 July, 2011.
7. The Committee, at their sitting held on 8 December, 2011 considered and adopted this Report.

336 337

8. The Committee wish to express their thanks to the officials of the Ministry of Planning and the Unique Identification Authority of India (UIDAI) for furnishing the requisite material and information which were desired in connection with the examination of the Bill. The Committee would also thank all the institutions and experts for their valuable suggestions on the Bill.

9 For facility of reference, the observations/recommendations of the Committee have been printed in thick type in the body of the Report.

New Delhi;
9 December, 2011
20 Aghrayana, 1938(Saka)

YASHWANT SINHA,
Chairman,
Standing Committee on Finance

REPORT

PART - I

237
338

A. Introduction

1. With a view to ensure that the benefits of centrally sponsored schemes reaches to right person and not misused, the Central Government had decided to issue unique identification numbers to all residents in India and to certain other persons. The scheme of unique identification involves collection of demographic and biometric information from individuals for the purpose of issuing of unique identification numbers to such individuals. The Central Government, for the purpose of issuing unique identification numbers, constituted the Unique Identification Authority of India (UIDAI) on 28th January, 2009, being executive in nature, which is at present functioning under the Planning Commission
2. It has been observed and assessed by the Government that the issue of unique identification numbers may involve certain issues, such as (a) security and confidentiality of information, imposition of obligation of disclosure of information so collected in certain cases, (b) impersonation by certain individuals at the time of enrolment for issue of unique identification numbers, (c) unauthorised access to the Central Identities Data Repository (CIDR), (d) manipulation of biometric information, (e) investigation of certain acts constituting offence, and (f) unauthorised disclosure of the information collected for the purpose of issue of unique identification numbers, which should be addressed by law and attract penalties.
3. In view of the foregoing paragraph, the Government has felt it necessary to make the said Authority as a statutory authority for carrying out the functions of issuing unique identification numbers to the residents in India and to certain other persons in an effective manner. It is, therefore, proposed to enact the National Identification Authority of India Bill, 2010 to provide for the establishment of the National Identification Authority of India (NIDAI) for the purpose of issuing identification numbers (which has been referred to as aadhaar number) to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access

339
~~338~~

to benefits and services to which they are entitled and for matters connected therewith or incidental thereto.

B. Objectives and Salient Features of the Bill

4. The National Identification Authority of India Bill, 2010, introduced in Rajya Sabha on 3rd December, 2010, *inter alia*, seeks to provide—

(a) for issue of aadhaar numbers to every resident by the Authority on providing his demographic and biometric information to it in such manner as may be specified by regulations;

(b) for authentication of the aadhaar number of an aadhaar number holder in relation to his demographic and biometric information subject to such conditions and on payment of such fees as may be specified by regulations;

(c) for establishment of the National Identification Authority of India consisting of a Chairperson and two part-time Members;

(d) that the Authority to exercise powers and discharge functions which, *inter alia*, include —

(i) specifying the demographic and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof;

(ii) collecting demographic and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations;

(iii) maintaining and updating the information of individuals in the CDR in such manner as may be specified by regulations;

(iv) specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations;

(e) that the Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health;

(f) that the Authority may engage one or more entities to establish and maintain the CDR and to perform any other functions as may be specified by regulations;

(g) for constitution of the Identity Review Committee consisting of three members (one of whom shall be the chairperson) to ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage

of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government;

(h) 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 CIDR) is secured and protected against any loss or unauthorized access or use or unauthorized disclosure thereof; and

(i) for offences and penalties for contravention of the provisions of the proposed legislation.

C. Evolution of the UIDAI

5. The concept of a Unique Identification (UID) scheme was first discussed and worked upon since 2006 when administrative approval for the scheme 'Unique ID for BPL families' was given on 3rd March, 2006 by the Department of Information Technology, Ministry of Communications and Information Technology.

6. Subsequently, a Processes Committee was set up on 3rd July, 2006 to suggest processes for updation, modification, addition and deletion of data fields from the core database to be created under the said project. The Committee appreciated the need of a UID Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the Authority.

7. Thereafter, since the Registrar General of India was engaged in the creation of the National Population Register (NPR) and issuance of Multi-purpose National Identity Cards to citizens of India, it was decided with the approval of the Prime Minister, to constitute an Empowered Group of Ministers (EGoM) to collate the two schemes – the NPR under the Citizenship Act, 1955 and the UID scheme. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the scheme and take a final view on these. The EGoM was constituted on 4th December, 2006 and a series of meetings took place as follows:-

a) First meeting of EGoM: 22nd November, 2007 :

- Recognized the need for creating an identity related resident database regardless of whether the database is created based on a

340
341

de-novo collection of individual data or is based on already existing data such as the voter list.

- Need to identify and establish institutional mechanism that will own the database and be responsible for its maintenance.

b) Second meeting of EGoM: 28th January, 2008

- The proposal to establish UID Authority under the Planning Commission was approved.

c) Third meeting of EGoM: 7th August, 2008

- Referred certain matters raised with relation to the UIDAI to a Committee of Secretaries for examination

d) Fourth meeting of EGoM: 4th November, 2008

- It was decided to notify UIDAI as an executive authority. Decision on investing it with statutory authority would be taken up later.
- UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government

8. The UIDAI was constituted on 28th January, 2009 under the Chairmanship of Shri Nandan M. Nilekani as an attached office under the aegis of the Planning Commission. The UIDAI was *inter-alia* given the responsibility to lay down plan and policies to implement the UID scheme, own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis. The Prime Minister's Council of UIDAI and a Cabinet Committee on UIDAI (called CC-UIDAI) were set up on 30th July, 2009 and 22nd October, 2009 respectively for achieving the objectives of the Authority.

9. Asked why the matter of conferring statutory status to the UIDAI was deferred, the Ministry of Planning have submitted their written response as under:-

"Based on the proposal that formation of the UIDAI under the Planning Commission would ensure better coordination with different departments, it was decided that initially the UIDAI may be notified as an executive authority under the Planning Commission and the issue of investing the UIDAI with statutory authority and the reconciliation of such statutory role with National Registration Authority (NRA) can be considered at an appropriate time".

341
342

10. Justifying the extension of the UID scheme, which is initially intended for BPL families, to all residents and other categories of individuals, the Ministry of Planning in their written response have submitted as under:-

"The UID scheme was extended to all residents and other categories of individuals to gradually do away the *de novo* exercises each time for field level data collection. Simultaneously, it would also ensure that links to more and more identity based databases are created by inclusion of the UID number in their databases".

11. In this regard, Dr. R. Ramakumar, Expert, in his post-evidence reply has, among other things, added as follows:-

"...it has been proven again and again that in the Indian environment, the failure to enroll with fingerprints is as high as 15% due to the prevalence of a huge population dependent on manual labour. These are essentially the poor and marginalised sections of the society. So, while the poor do indeed need identity proofs, aadhaar is not the right way to do that..."

12. The Ministry in their written reply have stated, among other things, that :-

"While there may be a number of factors contributing to the failure to enroll (like geography, age groups, occupation etc) and the figures quoted..... may not hold good in all situations, failure to enroll is a reality ... For enrolment purpose, UIDAI has already built in processes to handle biometric exceptions."

D. Issuance of aadhaar numbers pending passing the Bill by Parliament

13. Justice Dr. M. Rama Jois, MP (Rajya Sabha) in his representation addressed to the Chairman, Standing Committee on Finance has *inter-alia* pointed out since the NIDAI Bill is pending for consideration before the Standing Committee on Finance, implementation of the provisions of the Bill, issue of aadhaar numbers and incurring expenditure from the exchequer by the Government is a clear circumvention of Parliament, and therefore, should be kept in abeyance awaiting debate in and decision of both Houses of Parliament.

14. On being asked about the legal basis under which the UIDAI is functioning at present, and the mechanism that the UIDAI has adopted, since its inception, to deal with any of the issues like security and confidentiality of

343.
347-
information and other offences related to issue of the aadhaar numbers, the Ministry of Planning in a written reply have *inter-alia* stated that:-

"....The matter about commencement of operation of the UIDAI before a legal framework was put in place was referred to the Ministry of Law & Justice wherein opinion was sought on the issue whether in absence of a specific enabling law, would there be any constraints in collecting the data (including biometrics) and in issuing the UID numbers to residents in accordance with the mandate given to the Authority. The Ministry of Law & Justice, after examining the matter, had mentioned that it is a settled position that powers of the Executive are co-extensive with the legislative power of the Government and that the Government is not debarred from exercising its executive power in the areas which are not regulated by specific legislation. It had also been opined that till the time such legislation is framed the Authority can continue to function under the executive order issued by the Government and the scheme that may be prepared by the UIDAI. It was also opined that the Authority can collect information/data for implementation of the UID scheme. Such implementation can be done by giving wide publicity to the scheme and persuading the agencies/individual to part with necessary information

The UIDAI has not faced issues such as breach of security and confidentiality, manipulation of biometrics, unauthorized access to the CIDR or other related offences since its inception.....till the time Parliament passes the Bill, these matters will be covered by the relevant laws".

15. The opinion of the Attorney-General of India on the above mentioned issues as obtained by the Ministry of Law & Justice (Department of Legal Affairs) is furnished below -

"The competence of the Executive is not limited to take steps to implement the law proposed to be passed by Parliament. Executive Power operates independently. The Executive is not implementing the provisions of the Bill. The Authority presently functioning under the Executive Notification dated 28th January, 2009 is doing so under valid authority and there is nothing in law or otherwise which prevents the Authority from functioning under the Executive Authorisation.

The power of Executive is clear and there is no question of circumventing Parliament or the Executive becoming a substitute of Parliament. On the contrary, what is sought to be done is to achieve a seamless transition of the authority from an Executive Authority into a statutory authority.

All the expenditure which is being incurred is sanctioned by Parliament in accordance with the financial procedure set forth in the Constitution. If the Bill is not passed by any reason and if Parliament is of the view that

10. Justifying the extension of the UID scheme, which is initially intended for BPL families, to all residents and other categories of individuals, the Ministry of Planning in their written response have submitted as under:-

"The UID scheme was extended to all residents and other categories of individuals to gradually do away the *de novo* exercises each time for field level data collection. Simultaneously, it would also ensure that links to more and more identity based databases are created by inclusion of the UID number in their databases".

11. In this regard Dr. R. Ramakumar, Expert, in his post-evidence reply has, among other things, added as follows:-

" it has been proven again and again that in the Indian environment, the failure to enroll with fingerprints is as high as 15% due to the prevalence of a huge population dependent on manual labour. These are essentially the poor and marginalised sections of the society. So, while the poor do indeed need identity proofs, aadhaar is not the right way to do that... "

12. The Ministry in their written reply have stated, among other things, that :-

"While there may be a number of factors contributing to the failure to enroll (like geography, age groups, occupation etc.) and the figures quoted ... may not hold good in all situations, failure to enroll is a reality. For enrolment purpose, UIDAI has already built in processes to handle biometric exceptions."

D. Issuance of aadhaar numbers pending passing the Bill by Parliament

13. Justice Dr. M. Rama Jois, MP (Rajya Sabha) in his representation addressed to the Chairman, Standing Committee on Finance has *inter-alia* pointed out since the NIDAI Bill is pending for consideration before the Standing Committee on Finance, implementation of the provisions of the Bill, issue of aadhaar numbers and incurring expenditure from the exchequer by the Government is a clear circumvention of Parliament, and therefore, should be kept in abeyance awaiting debate in and decision of both Houses of Parliament.

14. On being asked about the legal basis under which the UIDAI is functioning at present, and the mechanism that the UIDAI has adopted, since its inception, to deal with any of the issues like security and confidentiality of

343.
342
information and other offences related to issue of the aadhaar numbers, the Ministry of Planning in a written reply have *inter-alia* stated that:-

"....The matter about commencement of operation of the UIDAI before a legal framework was put in place was referred to the Ministry of Law & Justice wherein opinion was sought on the issue whether in absence of a specific enabling law, would there be any constraints in collecting the data (including biometrics) and in issuing the UID numbers to residents in accordance with the mandate given to the Authority. The Ministry of Law & Justice, after examining the matter, had mentioned that it is a settled position that powers of the Executive are co-extensive with the legislative power of the Government and that the Government is not debarred from exercising its executive power in the areas which are not regulated by specific legislation. It had also been opined that till the time such legislation is framed the Authority can continue to function under the executive order issued by the Government and the scheme that may be prepared by the UIDAI. It was also opined that the Authority can collect information/data for implementation of the UID scheme. Such implementation can be done by giving wide publicity to the scheme and persuading the agencies/individual to part with necessary information.

The UIDAI has not faced issues such as breach of security and confidentiality, manipulation of biometrics, unauthorized access to the CIDR or other related offences since its inception...till the time Parliament passes the Bill, these matters will be covered by the relevant laws".

15. The opinion of the Attorney-General of India on the above mentioned issues as obtained by the Ministry of Law & Justice (Department of Legal Affairs) is furnished below:-

"The competence of the Executive is not limited to take steps to implement the law proposed to be passed by Parliament. Executive Power operates independently. The Executive is not implementing the provisions of the Bill. The Authority presently functioning under the Executive Notification dated 28th January, 2009 is doing so under valid authority and there is nothing in law or otherwise which prevents the Authority from functioning under the Executive Authorisation.

The power of Executive is clear and there is no question of circumventing Parliament or the Executive becoming a substitute of Parliament. On the contrary, what is sought to be done is to achieve a seamless transition of the authority from an Executive Authority into a statutory authority.

All the expenditure which is being incurred is sanctioned by Parliament in accordance with the financial procedure set forth in the Constitution. If the Bill is not passed by any reason and if Parliament is of the view that

351
342

the Authority should not function and express its will to that effect, the exercise would have to be discontinued. This contingency does not arise.

The present Bill being implemented without Parliaments' approval does not set a bad precedent in the Parliamentary form of Government. On the contrary, the fact that the Authority is sought to be converted from an Executive Authority to a statutory authority, it underlines the supremacy of Parliament".

16. On this issue, Dr. Usha Ramanathan, Expert, in her post-evidence reply has *inter-alia* stated that:-

"Article 73 of the Constitution delineates the extent of executive power of the Union and describes it as extending to matters with respect to which Parliament has power to make laws. .

While the executive power of the Union, and of the States, is co-extensive with the legislative power of the Union and the States, this is a provision that sets out the limits of the power. These are not provisions that are meant to make Parliament, or the legislatures, redundant. While executive power cannot extend beyond the legislative power of the Union and the States, Parliament and the legislatures can, and routinely do, set out the terms on which the executive is to function. This is also how 'delegated legislation' or 'subordinate legislation' has to be within the extent of the 'parent statute'.....

It is a plain misconception to think that the executive can do what it pleases, including in relation to infringing constitutional rights and protections for the reason that Parliament and legislatures have the power to make law on the subject"

E. UID scheme

17. A resident who seeks to obtain an aadhaar number shall provide his / her demographic and biometric information to enrolling agencies appointed by Registrars. A resident who does not possess any documentary proof of identity or proof of address can obtain an aadhaar number by being introduced by an introducer.

18. The UIDAI has executed Memoranda of Understanding (MoU) with the partners including all the States and Union Territories, 25 financial institutions (including LIC) to act as Registrars for implementing the scheme. The roles and responsibilities of the partners flow from the MoU.

345
344

19. The UIDAI requires only basic identity data such as name, age, gender, address and relationship details in case of minors, for issue of unique identity number. This is commonly known as 'Know your Resident' (KYR). The partner registrars are using this resident interface as an opportunity to update their own selected data bases such as ration card number, MGNREGS job card number, PAN card etc. This is commonly known as 'Know your Resident Plus' (KYR+). Collection of these information is purely an initiative of respective Registrars and not mandatory for issue of aadhaar number.

20. The UIDAI is collecting bare minimum demographic information from the residents; any other kind of information, viz., rural, semi-urban and urban areas, persons with disabilities, migrant unskilled and unorganized workers, nomadic tribes and others who do not have any permanent dwelling house, is not available with UIDAI. Asked how the coverage of marginalized sections of population, without having the data of aadhaar numbers issued to them, could be achieved, the Ministry has submitted that the Authority proposes to cover the marginalized and poor sections of the population through special enrolment camps organized for them.

21. In a news item dated 6th September, 2011, it has been reported that the Ministry of Home Affairs have identified flaws in the enrolment process followed by the UIDAI, citing cases where people have got aadhaar numbers on the basis of false affidavits.

22. Further, an expert has brought to the notice of the Standing Committee on Finance that issues of liability and responsibility for maintaining accuracy of data on the Register, conducting identity checks and ensuring the integrity of the overall operation of the UID scheme have not been resolved. On being asked to comment on this, the Ministry of Planning have submitted a written reply as follows:-

".....Registrars have to put processes in place to ensure that the data collected is accurate. It is also the responsibility of the Registrars to appoint verifiers (for verifying the documents presented by the resident) and introducers to handle cases where the residents do not have any documents".

23. It has been reported in a news item that the Ministry of Home Affairs have alleged that some of the registrars have not adhered to the laid down procedures under UIDAI. It has also been noticed that the Government of Kerala vide G.O.(MS)No:16/2011/ITD dated 3rd June, 2011 has *inter-alia* stated that the MoU was signed between UIDAI and Government of Kerala for implementation of the UID project subject to condition that the clauses on the standards, protocol, criteria etc. in the MoU shall be in accordance with the State IT policy

F. Global Experience

24. It has been brought to the notice of the Standing Committee on Finance that on the basis of the findings of London School of Economics (LSE) report, the Government of United Kingdom has abandoned its ID project (repealed its Identity Cards Act, 2006) citing a range of reasons, which includes high cost, unsafe, untested and unreliable technology, and the changing relationship between the state and the citizen etc.

To a specific issue of relevance of any of the above mentioned factors in the Indian context, it has been informed by the Ministry as follows:-

"There are significant differences between the UK's ID card project and the UID project and to equate the two would not be appropriate. The differences are as follows:-

a) The UK system involved issuing a card which stored the information of the individual including their biometrics on the card. UID scheme involves issuing a number. No card containing the biometric information is being issued. UK already has the National insurance number which is used often as a means to verify the identity of the individual.

b) The statutory framework envisaged made it mandatory to have the UK ID card. Aadhaar number is not mandatory.

c) The data fields were large and required the individual to provide accurate information of all other ID numbers such as driver's license, national insurance number and other such details thereby linking the UK ID card database to all other databases on which the individual was registered. UID Scheme collects limited information and the database is not linked to other databases.

347
346

d) In UK, the legislative framework and structure approached it from a security perspective. The context and need in India is different. The UID scheme is envisaged as a mean to enhance the delivery of welfare benefits and services".

25. When asked as to whether any analysis has been carried out on the experience of countries where National IDs are in use as well as countries where it has been discontinued, the Ministry have *inter-alia* informed the Committee in a written reply as follows:-

"In some countries the use of smart cards to store significant data about the resident added to concerns about ID fraud and duplication ...

The comparisons between developed countries, which are looking at additional ID forms from a security perspective, versus India, a developing country which, like Brazil and Mexico, is attempting to, build the basic identity and verification infrastructure essential to delivering welfare benefits, and promoting inclusive growth, is not a reasonable one".

G. Existing identity forms vs need for aadhaar number

26. A view has been expressed that adding another form of identity (i.e. aadhaar number) without studying the possibility of using the existing forms of identity, for example, Voter ID card, to solve the current problems appears to be a waste of resources.

27. The Ministry of Planning in a written submission have *inter-alia* stated the following:-

".....in the current framework there is no single document which is uniformly acceptable as proof of identity across India – irrespective of age, gender and familial connections. Establishing identity is a challenge for the poor, particularly when they move from place to place as a consequence lack of proof of identity makes it difficult for the poor to access benefits and services.

.....Aadhaar number is an enabler..... The benefits of aadhaar number are:-

"For residents: The aadhaar number will become the single source of identity verification. Once residents enroll, they can use the number multiple times -- they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on... the number will also give migrants mobility of identity.

347
348

For Registrars and enrollers: The UIDAI will only enroll residents after de-duplicating records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower Know Your Resident (KYR) costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate. The strong authentication that the aadhaar number offers will improve services, leading to better resident satisfaction.

For Governments: Eliminating duplication under various schemes is expected to save the Government exchequer a substantial amount. It will also provide Governments with accurate data on residents, enable direct benefit programs, and allow Government departments to coordinate investments and share information".

28. The Ministry have further added that:

"....reason for starting the project is not for overriding existing Ids.....All the above documents are relevant to a domain and for a service. Aadhaar number is to be used as a general proof of identity and proof of address".

H. Identity and Eligibility

29. According to a news item dated 7th July, 2011, the operationalisation of aadhaar, the unique identification number, will make it possible to link entitlements to targeted beneficiaries. But it will not ensure beneficiaries have been correctly identified. Thus, the old problem of proper identification that bedevils the present system will continue.

30. It has also been brought to the notice of the Standing Committee on Finance that a key issue in targeted welfare schemes is said to be of eligibility and not identity. Government entitlements are unavailable to the poor, primarily due to the eligibility determination process having many loopholes and lacunae. One identity like aadhaar number has nothing to do with such entitlements.

31. Asked to furnish comments, the Ministry of Planning in a written reply have stated that-

"....With aadhaar number integration in various Government schemes, the identity of the beneficiary gets established, by which it is ensured that the government scheme benefits reach the intended beneficiaries. Availability of identity and eligibility information together provides an important tool to plug the loopholes in the eligibility determination process, and in managing the eligibility life cycle for a beneficiary".

348
349

32. Dr. Reetika Khera, Expert, while deposing before the Committee has *inter-alia* stated as follows:-

".....exclusion is more on account of poor coverage of these schemes. Say, for instance, in the Public Distribution System, the Planning Commission says that only 'x' per cent of the rural population will get the BPL cards and because of that cap that is set at the Central level, we find that lots of people are excluded".

I. Aadhaar Number and National Population Register (NPR)

33. The Standing Committee on Finance, during briefing on the Bill held on 11th February, 2011, raised *inter-alia* the issue of possibility of dovetailing the UID exercise with the census operation. In this regard, the Ministry of Planning in their written reply have, among other things, stated as follows:-

"the UIDAI is adopting a multiple registrar approach and the Registrar General of India (RGI) will be one of the Registrars of the UIDAI. To synergize the two exercises, an Inter Ministerial Coordination Committee has been set up to minimize duplication. The UIDAI is making all efforts to synergize with National Population Register (NPR) exercise....".

34. According to a news item dated 6th September, 2011, the Ministry of Home Affairs said that it would not be preferable to rely entirely on private sector players' for biometric enrolments into the NPR since the population register will form the basis on which citizenship would be determined in the future. Unlike the UIDAI system, the NPR system follows an elaborate procedure to verify and cover the entire population of every area, and the data collected is subjected to 'social vetting' and accountability can be fixed under the NPR system.

35. In an another news article it has been reported that while registration to the NPR is compulsory and a National Identity Number is linked to each name, the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 does not approve of linking biometrics with personal information. However, according to, the annual reports of the Ministry of Home Affairs, it said that integration of photographs and finger biometrics of 17.2 lakh out of 20.6 lakh records has been completed.

350
349

J. Coordination between the agencies involved in the UID scheme

36. In a detailed note on the NIDAI Bill, the Ministry of Planning have *inter-alia* submitted that -

"Implementation of a project of this size is challenging. It involves co-ordination with multiple stakeholders and effective monitoring of implementation at every level....".

37. The Ministry of Finance (Department of Expenditure), however, while commenting on embedding aadhaar numbers in databases to enable interaction have stated that:-

"It must be done urgently by single agency, perhaps NPR. Cabinet has approved (22.7.2010) outlay of Rs. 3,023.01 crore *inter-alia* for assistance for Information Communication Technology (ICT) infrastructure of Rs. 450 crore for integrating/ synergizing Aadhaar numbers with existing databases. Concerned about lack of co-ordination leading to duplication effort and expenditure with at least 6 agencies collecting information (NPR, MNREGA, BPL Census, UID, RSBY and Bank Smart Cards)".

38. It has been reported in a news item dated 3rd October, 2011 that the UID project has become focus of the ire of various arms of the government for rather disparate reasons. Asked to furnish the comments on the said news item, the Ministry of Planning have submitted a written reply as follows:-

| Views reported in the news item | Comments of the Ministry of Planning |
|---|---|
| ..the Finance Ministry rejected UIDAI's request for Rs.14,000 crore expenditure programme. | It is not correct that the Finance Ministry have rejected the budget expenditure. The proposal for phase III has been recommended by the EFC on 15 September, 2011 after optimizing the cost estimates with certain stipulations to be complied with by the UIDAI to achieve economy of scales, avoid duplication and avail convergence in the programme. |
| ..the planning commission too jumped into the fray, suddenly awakening to the deficiency in the structure and functioning of the Authority. | Aadhaar programme is a complex project of its kind launched first time in the country. EFC is an Inter-Ministerial forum to appraise the proposal rigorously to facilitate decision making by the Competent Authority. Planning Commission is one of the nodal appraising agencies to the EFC forum. On approval by |

351
350

| | |
|--|--|
| | <p>Planning Commission some issues regarding design parameters, cost estimates and manner of implementation were emerged, which could not be visualized at project formulation stage. These issues have been deliberated in the EFC meeting and resolved through certain stipulations to be adhered to by UIDAI during execution of the project.</p> |
| <p>Adding to the confusion were the apparently negative comments made by the Ministry of Home Affairs(MHA) on the flaws in the enrolment process and the security of the biometric data. The Home Ministry's apparently nervous of the UIDAI's efforts to extend its aadhaar enrolment mandate, as the office of the Registrar General of India, an arm of the Ministry, is simultaneously compiling a National Population Register (NPR) which is a comprehensive identity database, as a part of the 2011 census operations currently under way.</p> | <p>While responding to the EFC memo of the UIDAI, the RG! (MHA) have observed as follows -</p> <p>A security audit of the entire process of UIDAI including enrolment process in UIDAI, the enrolment software, data storage, data management, etc should be conducted by an appropriate agency.</p> <p>The Comments of the UIDAI on this are:-</p> <p>UIDAI is developing a monitoring and evaluation framework to provide a comprehensive mechanism for continuously monitoring and evaluating the UIDAI program. Considering that a formal structured monitoring and evaluation framework will form the cornerstone for measuring the outcome of UIDAI programme, a distinct component 'Monitoring and evaluation' has been included in the current EFC proposal. Some of the audits planned on a periodic basis are:- (i) Enrolment Client Audit; (ii) Enrolment Process (Field) Audits; (iii) ASDMSA Application Audits; (iv) Authentication User Agency Audits; (v) Data Center Audits; (vi) Security Audits; (vii) Impact Assessment (Grants in Aid for Research); and (viii) Other Third Party Audit Services.</p> |
| <p>The confusion about the turf of UIDAI and the MHA is rather surprising,</p> | <p>UIDAI has no comments to offer.</p> |

| | |
|--|---|
| <p>given the fact that an EGoM was constituted as early as 2006 to collate the two schemes, namely the NPR and the unique identification number, as aadhaar was then known.</p> | |
| <p>RBI made the waters murkier by first going against the Finance Ministry notification that was issued in 2010 to permit the use of Know Your Customer (KYC) norms- by limiting the use of aadhaar numbers to "small accounts". It then retracted, by allowing use of aadhaar numbers to all bank accounts without any limitations, but only after again insisting that the banks must satisfy themselves about the current address of the customer. RBI's reluctance to fully accept the aadhaar numbers for the KYC norms is surprising, given that more than a dozen leading banks in the country are partnering with UIDAI to deliver aadhaar numbers to the citizens, and also when the aadhaar number have been accepted by the insurance companies and SEBI for meeting KYC norms.</p> | <p>It is clarified that-</p> <p>(i) aadhaar is sufficient KYC for opening all bank accounts now. This includes no-frill accounts- as per Reserve Bank's circular dated January 27, 2011 – and any bank account as per September 28, 2011 circular.</p> <p>(ii) Banks may ask for additional proof of residence if the current residence is not the same as the address given on the aadhaar document. This procedure is consistent with bank policies applicable to all other officially valid documents including passport, driving license and is not specific to aadhaar</p> |

K. Civil Liberties Perspective

39. In a detailed note on the Bill, the Ministry of Planning have stated that issues like access and misuse of personal information, surveillance, profiling, prohibiting other data bases from storing aadhaar numbers; and securing confidentiality of information which is in the registrars domain need to be addressed in larger data protection legislation. In this connection, the Ministry have been asked to comment on the view that the Bill in its current form appears to be unsafe in law as there is no law at present on privacy, and data protection, therefore, it would be appropriate to consider the Bill for legislation only after passing the legislation on privacy, and data protection so as to ensure that there is no conflict between these laws. The Ministry in a written reply have *inter-alia* stated as under:-

353
352

"UIDAI has taken appropriate steps to ensure security and protection of data under this law and has incorporated data protection principles within its policy and implementation framework.....

Since appropriate steps have been taken, there is no dependency on the general data protection law. ...when the data protection framework comes into place the Authority will follow the same since a national data protection law will apply to all agencies and institutions collecting information.

Collection of information without a privacy law in place does not violate the right to privacy of the individual....There is no bar on collecting information, the only requirement to be fulfilled with respect to the protection of the privacy of an individual is that care should be taken in collection and use of information, consent of individual would be relevant, information should be kept safe and confidential..

.....The proposed Privacy law should also seek to strike a balance between the legitimate demands of protecting individual liberties while recognizing the need for larger public interest to prevail in certain well defined circumstances".

40. Responding to a suggestion received from PRS Legislative Branch that the existence of a unique identifier may facilitate record linkages across separate databases, the Ministry in a written reply have submitted that issues of linking and matching of databases need to be addressed through a data protection legislation which is currently being considered by the Department of Personnel.

41. The National Human Rights Commission (NHRC), on being asked to comment on the implications of the provisions of the Bill on the individual's right to privacy, has *inter alia* informed the Committee in their post-evidence reply as follows:-

....the right to privacy presupposes that such information relating to an individual which he would not like to share with others will not be disclosed. It may be mentioned that the right of privacy is not an absolute right.. ..."

42. On the same issue, Dr. Jsha Ramanathan, expert in her post-evidence reply has stated that:-

"....The right to dignity, the right to privacy, personal security and safety, the protection against surveillance, are constitutionally protected. The production of a number accompanied by the use of methods such as fingerprinting and iris scanning is even more invasive than is permitted to be applied to a leged offenders. Article 20 (3) provides protection against

354
353

compulsory extraction of personal information. Denying services, and rights, to persons because they are unwilling to part with the information in a manner that is more than likely to result in convergence and commodification of their personal information, surveillance, profiling, tagging and tracking is compulsory extraction that clearly reduces the constitutional rights of an ordinary citizen to less than that of an alleged offender. And that this is being done without the protection of law renders the exercise, per se, illegal. Apart from its 'uses', the potential for abuse is undeniable. In a similar context, another court – the Philippines Supreme Court – said:the data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to misuse, a temptation that may be too great for some of our authorities to resist".

L. Financial Implications

(i) Feasibility Study

43 The Ministry of Planning in a detailed note on the Bill have stated that aadhaar number is cost-effective compared to other alternate targeted solutions to the problems identified in delivering services and benefits such as eliminating duplicate and fake identities. The Detailed Project Report (DPR) of the UID scheme has been prepared and submitted by M/s Ernst & Young Pvt.Ltd. in April, 2011.

44. Asked whether any committee has been set up to study the financial implications of the UID scheme; and also to furnish the details of feasibility study carried out, if any, covering all aspects of the UID scheme such as setting up of the proposed NIDAI, and cost-benefit analysis, the Ministry in a written reply have, among other things, submitted that:-

"No committee has been set up to study the financial implications of the UID scheme. As per laid down guidelines/procedure the Expenditure Finance Committee (EFC) reviews project proposals and its financial implications wherein the views of all stakeholders/ministries are taken in to account...

.....deliberations were held with all relevant stakeholders including Planning Commission, Registrar General of India, Election Commission of India, Ministry of Rural Development, Ministry of Urban Development and State Governments. A Proof of Concept study was undertaken in the States of Gujarat, Karnataka, U.P. and Orissa in four rural and one urban locations to establish the feasibility of linking UID with partner-databases and to validate the possibility of one-time linkage which once

355
354

established would be maintained on an ongoing basis by the UIDAI. An assessment study was carried out in 10 Central Ministries and their respective departments in four states (Karnataka, Uttar Pradesh, Gujarat and West Bengal).

(ii) Estimated cost of the UID scheme

45. The UID scheme is a Central Sector Scheme. The estimated cost of the Phase-I and Phase-II of the scheme spread over five years is Rs.3170.32 crore (Rs.147.31 crore for Phase-I and Rs.3023.01 crore for Phase-II). The estimated cost includes scheme components for issue of 10 crore UID numbers by March, 2011 and recurring establishment costs for the entire scheme up to March, 2014. The Budget for Phase-III of the scheme to the tune of Rs.8861 crore has been approved.

46. According to news items, the total cost of the UID scheme may run up to Rs. 1,50,000 crore. Even after the commitment of such levels of expenditures, the uncertainty over the technological options and ultimate viability of the scheme remains.

(iii) Comparative cost of aadhaar number and existing ID documents

47. Asked to furnish the details of comparative cost of existing ID documents (per individual), namely, Voter Id card, PAN card, driving license and aadhaar number, the Ministry has *inter-alia* informed the Committee in a written reply that the comparative costs of the documents mentioned above are not available.

(iv) Funding of other biometric projects

48. It is noticed that a project namely, Bharatiya - Automated Finger Print Identification System (AFSI), was launched in January, 2009, being funded by the Department of Information Technology, Ministry of Communications and Information Technology, for collection of biometric information of the people of the country.

49. Asked to clarify as to whether the biometric information (finger prints) being collected under the Bharatiya - AFSI project could also be used by the UIDAI, the Ministry have submitted that-

356
355

"The biometrics required for the aadhaar project are iris, ten finger prints and photograph. To ensure uniqueness of the individual, it is essential that the biometrics captured are as per the specifications laid down by the Biometrics Standards Committee. The quality, nature and manner of collection of biometric data by other biometric projects may not be of the nature that can be used for the purpose of the aadhaar scheme and hence it may not be possible to use the fingerprints captured under the Bhartiya-AFSI project".

(v) **Revenue model of the UIDAI**

50. According to a detailed note on the bill furnished by the Ministry of Planning, demographic data and address verification will be provided free of cost till a separate pricing policy is announced in due course.

51. However, in a news item dated 6th September, 2011, it has been reported that the Ministry of Home Affairs pointed out uncertainties in the UIDAI's revenue model.

M. Technology

52. The Biometrics Standards Committee set up by the UIDAI has recognized in its report that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts. It has further noted that it is:

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

53. Asked to explain the reliability of technical architecture of the UID scheme, the Ministry of Planning in a detailed note on the NIDAI Bill have, among other things, stated as follows:-

"The UID project is a complex technology project. Nowhere in the world has such a large biometric database of a billion people being maintained. The frontiers of technology in biometrics are being tested and used in the project.....

The technical architecture of the UID scheme is at this point, is based on high-level assumptions. The architecture has been structured to

356
357

ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security.....

The project team is learning and adapting to the challenges and ensuring that the solutions that are being offered are the best in the world to achieve the task....".

54. Further asked as to given the high degree of assumptions on the reliability of technology adopted by the UIDAI and probability of system failures of different degrees, whether incurring huge costs on the UID scheme is prudent and affordable, the Ministry have stated in a written reply, among other things, as follows:-

".....UIDAI is cognizant of the fact that biometric matching (which is a patterns matching) by its very nature will suffer from inaccuracy. However, these inaccuracy levels are less than 1%. This cannot be a reason for not attempting to use the technology.

It is well acknowledged that there will be failures in authentication for various reasons. After Proof of Concept studies on authentication, appropriate policies and processes will be developed to take care of situations where failure occurs for various reasons.....The choice of using the authentication services is left to the third party service provider.....Concerned agencies will have to develop policies and procedures to handle such exceptional situations. ... "

55. In a news article, one of the representatives of the UIDAI has admitted that the quality of fingerprints is bad because of the rough exterior of fingers caused by hardwork, and this poses a challenge for later authentication.

N. National Security vs the UID scheme

(i) Illegal residents

56. A concern over the possibility of illegal residents getting aadhaar numbers, and the safeguards in this regard has been raised by the Standing Committee on Finance during the sitting held on 11 February, 2011. In a written reply, the Ministry of Planning have stated as under:-

"Aadhaar number is not a proof of citizenship or domicile [Clause 6 of the Bill]. It only confirms identity and that too subject to authentication [Clause 4(3)]. This is clearly mandated in the NIDAI Bill and the communication being sent to the resident.

It is the responsibility of the Registrars to enrol a resident after due verification as per the procedure laid down by the UIDAI. If a person is not a resident as per the Bill, the Authority is being vested with the power

358
~~357~~

to omit/deactivate the aadhaar number [Clause 23 (2) (g)]. Subsequent attempts to enter the system can be detected"

(ii) Involvement of Private agencies

57. On the issue of security of proposed data of UIDAI, an unstarred question (no.2989) was raised in Rajya Sabha. The Minister of State in the Ministry of Planning and Minister of State in the Ministry of Parliamentary Affairs tabled the answer to the above said question in Rajya Sabha on 22 April, 2010 as follows:-

"National Informatics Centre (NIC) had pointed out that the issues relating to privacy and security of UID data, in case the data is not hosted in a Government data centre may be taken into consideration.

UIDAI is of the opinion that the hosting of data in a private data centre does not necessarily lead to a violation of privacy or security. Appropriate contractual arrangement shall be put in place with the data centre space provider to ensure security and privacy of the data.

At present, UIDAI does not have its own permanent facility to house its data centre. Therefore, 75 sq.ft of data centre space has been hired from M/s. ITI Ltd. for proof of concept and pilot on a rental basis".

58. The Ministry of Home Affairs, according to a news item, have questioned the security of citizens' biometric data in UIDAI's 'outsourced service oriented infrastructure' model.

59. To a specific query as to could outside agencies be allowed to partake in the UID scheme when doubts have been expressed on possible compromise with the interests of the national security, the Ministry of Planning in a written reply have *inter alia* stated that:-

"....the UIDAI has followed government procurement process and engaged the appropriate agencies for the implementation of the UID scheme....The UIDAI has also implemented a comprehensive information security policy....."

60. It is, however, reported in various news articles as late as dated 26th November, 2011 that controversies between the Ministry of Home Affairs and the UIDAI over the issues such as manner and processes followed by the UIDAI, duplication of efforts between National Population Register and aadhaar, and security of data remain unresolved.

358 359

PART - II

OBSERVATIONS / RECOMMENDATIONS

1. The Committee have carefully examined the written information furnished to them and heard the views for and against the National Identification Authority of India (NIDAI) Bill from various quarters such as the Ministry of Planning, the Unique Identification Authority of India (UIDAI), the National Human Rights Commission (NHRC) and experts. The clearance of the Ministry of Law & Justice for issuing aadhaar numbers, pending passing the Bill by Parliament, on the ground that powers of the Executive are co-extensive with the legislative power of the Government and that the Government is not debarred from exercising its Executive power in the areas which are not regulated by the legislation does not satisfy the Committee. The Committee are constrained to point out that in the instant case, since the law making is underway with the bill being pending, any executive action is as unethical and violative of Parliament's prerogatives as promulgation of an ordinance while one of the Houses of Parliament being in session.

2. The Committee are surprised that while the country is on one hand facing a serious problem of illegal immigrants and infiltration from across the borders, the National Identification Authority of India Bill, 2010 proposes to entitle every resident to obtain an aadhaar number, apart from entitling such other category of individuals as may be notified from time to time. This will, they apprehend, make even illegal immigrants entitled for an aadhaar number. The Committee are unable to understand the rationale of expanding the scheme to persons who are not citizens, as this entails numerous benefits proposed by the Government. The Committee have received a number of suggestions for restricting the scope of the UID scheme only to the citizens and for considering better options available with the Government by issuing Multi-Purpose National Identity Cards (MNICs) as a more acceptable alternative.

3. The Committee observe that *prima facie* the issue of unique identification number, which has been referred to as “aadhaar number” to individuals residing in India and other classes of individuals under the Unique Identification (UID) Scheme is riddled with serious lacunae and concern areas which have been identified as follows:-

- (a) The UID scheme has been conceptualized with no clarity of purpose and leaving many things to be sorted out during the course of its implementation; and is being implemented in a directionless way with a lot of confusion. The scheme which was initially meant for BPL families has been extended for all residents in India and to certain other persons. The Empowered Group of Ministers (EGoM), constituted for the purpose of collating the two schemes namely, the UID and National Population Register(NPR), and to look into the methodology and specifying target for effective completion of the UID scheme, failed to take concrete decision on important issues such as (a) identifying the focused purpose of the resident identity database; (b) methodology of collection of data; (c) removing the overlapping between the UID scheme and NPR; (d) conferring of statutory authority to the UIDAI since its inception; (e) structure and functioning of the UIDAI; (f) entrusting the collection of data and issue of unique identification number and national identification number to a single authority instead of the present UIDAI and its reconciliation with National Registration Authority;

(b) The need for conferring of statutory authority to the UIDAI felt by the Government way back in November, 2008, but was deferred for more than two years for no reason. In this regard, the Ministry of Planning have informed the Committee that till the time Parliament passes the NIDAI Bill, crucial matters impinging

29

361
360

on security and confidentiality of information will be covered by the relevant laws. The Committee are at a loss to understand as to how the UIDAI, without statutory power, could address key issues concerning their basic functioning and initiate proceedings against the defaulters and penalize them;

- As Amended
to Cm only
Ruh
- (c) The collection of biometric information and its linkage with personal information of individuals without amendment to the Citizenship Act, 1955 as well as the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003, appears to be beyond the scope of subordinate legislation, which needs to be examined in detail by Parliament;

- (d) Continuance of various existing forms of identity and the requirement of furnishing 'other documents' for proof of address, even after issue of aadhaar number, would render the claim made by the Ministry that aadhaar number is to be used as a general proof of identity and proof of address meaningless;

- (e) In addition to aadhaar numbers being issued by the UIDAI, the issuance of smart cards containing information of the individuals by the registrars is not only a duplication but also leads to ID fraud as prevalent in some countries; and

- Retention
to 1/2
- (f) The full or near full coverage of marginalized sections for issuing aadhaar numbers could not be achieved mainly owing to two reasons viz. (i) the UIDAI doesn't have the statistical data relating to them; and (ii) estimated failure of biometrics is expected to be as high as 15% due to a large chunk of population being dependent on manual labour.

4. The Committee regret to observe that despite the presence of serious difference of opinion within the Government on the UID scheme as illustrated below, the scheme continues to be implemented in an

362
361

overbearing manner without regard to legalities and other social consequences:-

(i) The Ministry of Finance (Department of Expenditure) have expressed concern that lack of coordination is leading to duplication of efforts and expenditure among at least six agencies collecting information (NPR, MGNREGS, BPL census, UIDAI, RSBY and Bank Smart Cards):

Threat to National Secy. //

(ii) The Ministry of Home Affairs are stated to have raised serious security concern over the efficacy of introducer system, involvement of private agencies in a large scale in the scheme which may become a threat to national security; uncertainties in the UIDAI's revenue model;

(iii) The National Informatics Centre (NIC) have pointed out that the issues relating to privacy and security of UID data could be better handled by storing in a Government data centre;

(iv) The Ministry of Planning have expressed reservation over the merits and functioning of the UIDAI; and the necessity of collection of iris image;

(v) Involvement of several nodal appraising agencies which may work at cross-purpose; and

(vi) Several Government agencies are collecting biometric(s) information in the name of different schemes.

5. The Committee are also unhappy to observe that the UID scheme lacks clarity on many issues such as even the basic purpose of issuing "aadhaar" number. Although the scheme claims that obtaining aadhaar number is voluntary, an apprehension is found to have developed in the minds of people that in future, services / benefits including food entitlements would be denied in case they do not have aadhaar number.

Threat to National Secy. //

362
363

It is also not clear as to whether possession of aadhaar number would be made mandatory in future for availing of benefits and services. Even if the aadhaar number links entitlements to targeted beneficiaries, it may not ensure that beneficiaries have been correctly identified. Thus, the present problem of proper identification would persist.

Waste

it is also not clear that the UID scheme would continue beyond the coverage of 200 million of the total population, the mandate given to the UIDAI. In case, the Government does not give further mandate, the whole exercise would become futile.

4.K. Shalve

6. Though there are significant differences between the identity system of other countries and the UID scheme, yet there are lessons from the global experience to be learnt before proceeding with the implementation of the UID scheme, which the Ministry of Planning have ignored completely. For instance, the United Kingdom shelved its Identity Cards Project for a number of reasons, which included:- (a) huge cost involved and possible cost overruns; (b) too complex; (c) untested, unreliable and unsafe technology; (d) possibility of risk to the safety and security of citizens; and (e) requirement of high standard security measures, which would result in escalating the estimated operational costs. In this context, the Report of the London School of Economics' Report on UK's Identity Project *inter-alia* states that ".....identity systems may create a range of new and unforeseen problems.....the risk of failure in the current proposals is therefore magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals". As these findings are very much relevant and applicable to the UID scheme, they should have been seriously considered.

Security

7. The UID scheme facilitates the UIDAI and the registrars to create database of information of people of the country. Considering the huge database size and possibility of misuse of information, the Committee are

of the view that enactment of national data protection law, which is at draft stage with the Ministry of Personnel, Public Grievances and Pensions, is a pre-requisite for any law that deals with large scale collection of information from individuals and its linkages across separate databases. In the absence of data protection legislation, it would be difficult to deal with the issues like access and misuse of personal information, surveillance, profiling, linking and matching of data bases and securing confidentiality of information etc.

8. The Committee note that the Ministry of Planning have admitted that (a) no committee has been constituted to study the financial implications of the UID scheme; and (b) comparative costs of the aadhaar number and various existing ID documents are also not available. The Committee also note that Detailed Project Report (DPR) of the UID Scheme has been done much later in April, 2011. The Committee thus strongly disapprove of the hasty manner in which the UID scheme has been approved. Unlike many other schemes / projects, no comprehensive feasibility study, which ought to have been done before approving such an expensive scheme, has been done involving all aspects of the UID scheme including cost-benefit analysis, comparative costs of aadhaar number and various forms of existing identity, financial implications and prevention of identity theft, for example, using hologram enabled ration card to eliminate fake and duplicate beneficiaries.

9. The Committee are afraid that the scheme may end up being dependent on private agencies, despite contractual agreement made by the UIDAI with several private vendors. As a result, the beneficiaries may be forced to pay over and above the charges to be prescribed by the UIDAI for availing of benefits and services, which are now available free of cost.

364 365

10. The Committee find that the scheme is full of uncertainty in technology as the complex scheme is built up on untested, unreliable technology and several assumptions. Further, despite adverse observations by the UIDAI's Biometrics Standards Committee on error rates of biometrics, the UIDAI is collecting the biometric information. It is also not known as to whether the proof of concept studies and assessment studies undertaken by the UIDAI have explored the possibilities of maintaining accuracy to a large level of enrolment of 1.2 billion people. Therefore, considering the possible limitations in applications of technology available now or in the near future, the Committee would believe that it is unlikely that the proposed objectives of the UID scheme could be achieved.

11. The Committee feel that entrusting the responsibility of verification of information of individuals to the registrars to ensure that only genuine residents get enrolled into the system may have far reaching consequences for national security. Given the limitation of any mechanism such as a security audit by an appropriate agency that would be setup for verifying the information etc., it is not sure as to whether complete verification of information of all aadhaar number holders is practically feasible; and whether it would deliver the intended results without compromising national security. As the National Identity Cards to citizens of India are proposed to be issued on the basis of aadhaar numbers, the possibility of possession of aadhaar numbers by illegal residents through false affidavits / introducer system cannot be ruled out.

12. The Committee take note that the Ministry of Home Affairs have alleged that some of the registrars have not adhered to the laid down procedures under UIDAI which renders the Memoranda of Understanding (MoU) signed between the UIDAI and the registrars meaningless; and it compromises the security and confidentiality of information of aadhaar

366
365

number holders. Even, according to the latest media reports, controversies between the Ministry of Home Affairs and the UIDAI over issues such as the manner and processes followed by the UIDAI, duplication of efforts between NPR and aadhaar, and security of data still remain unresolved.

13. In view of the afore-mentioned concerns and apprehensions about the UID scheme, particularly considering the contradictions and ambiguities within the Government on its implementation as well as implications, the Committee categorically convey their unacceptability of the National Identification Authority of India Bill, 2010 in its present form. The data already collected by the UIDAI may be transferred to the National Population Register (NPR), if the Government so chooses. The Committee would, thus, urge the Government to reconsider and review the UID scheme as also the proposals contained in the Bill in all its ramifications and bring forth a fresh legislation before Parliament.

New Delhi
11 December, 2011
20 Agrahayana, 1933 (Saka)

YASHWANT SINHA
Chairman,
Standing Committee on Finance

366 367

Appendix I

NOTE OF DISSENT

Shri Raashid Alvi, MP

I do not agree with the paragraph "13" of the draft Report on "The National Identification Authority of India Bill, 2010".

I suggest to delete "this para".

Sd/

Dated: 7 December, 2011

(RAASHID ALVI)

NOTE OF DISSENT

Prem Das Rai, MP

The National Identification Authority of India Bill, 2010

At the outset I do not believe that the bill should be rejected in the manner it has been. Since I have been inducted into the Committee recently I do not have the inputs that went in when the stakeholders and other Government departments were giving witness. I also do not know whether we gave enough time to the UID implementers to give evidence and present their point of view.

Hence, I would like to place on record that the issue of giving out Aadhaar numbers under the UID scheme, I believe, is one of the greatest import for social and economic inclusion in this country. I personally am privy to the kind of work that is needed at the grassroots as I was part of an organisation that did such work in the North East of India and other backward regions using some form of technology to bring in inclusion.

The linking of a person to a number and then being able to make give access to the right to that person is transformational. It is the next phase of transformation that technology can bring about in our own country. This has never been done anywhere in the world and we should be rightly proud of this.

I do agree there may be serious issues that need to be factored in which my esteemed colleagues have pointed out

I recommend that the Bill may be discussed in Parliament bringing about some of the changes so desired and do not concur that the Bill be brought fresh

Sd/-

(PREM DAS RAI)

Dated: 8 December, 2011

368
369

NOTE OF DISSENT

Manicka Tagore, MP

I could not attend this meeting on adoption of the draft report on the National Identification Authority of India Bill, 2010 because a very important discussion on the price rise was going on in the Lok Sabha. The Govt. of India with a view to ensure that the benefits of centrally sponsored schemes reaches to right persons and not misused, they had decided to issue unique identification numbers to all residents in India and to certain other persons the basic idea was to identification of the persons. The Ahar programme has been launched first time in India. The UIDAI officials have taken all possible precautions to make the exercise safe and secure. Both demographic and biometric data were collected and its method of collecting data were approved by the Demographic Standard and Verification Procedure Committee.

It is surprising to know that the committee members have not yet recognized the value of UID. This system will cut down fraud and corruption in every area of administration.

I dissent the observation and recommendation of the Standing Committee on Finance regarding the Draft Report on the National Identification Authority of India Bill, 2010. I request the Chairman that the UID bill may kindly be considered by the Government with our views and not rejected.

Dated 10 December, 2011

Sd/-
(MANICKA TAGORE)

370
369

Appendix II

MINUTES OF THE THIRTEENTH SITTING OF THE STANDING COMMITTEE ON FINANCE
(2010-11)

The Committee sat on Friday, the 11th February, 2011 from 1130 hrs to 1400 hrs.

PRESENT

Shri Yashwant Sinha – Chairman

MEMBERS

LOK SABHA

2. Shri. Bhartruhari Mahtab
3. Smt. Jaya Prada Nahata
4. Shri Rayapati Sambasiva Rao
5. Dr. Kavuru Sambasiva Rao
6. Shri Manicka Tagore

RAJYA SABHA

7. Shri S.S. Ahluwalia
8. Shri Raashid Alvi
9. Shri Piyush Goyal
10. Shri Moinul Hassan

SECRETARIAT

- | | | |
|---------------------------------|---|---------------------|
| 1. Shri A. K. Singh | – | Joint Secretary |
| 2. Shri T. G. Chandrasekhar | – | Additional Director |
| 3. Shri Ramkumar Suryanarayanan | – | Deputy Secretary |
| 4. Smt. B. Visala | – | Deputy Secretary |

WITNESSES

Ministry of Planning

1. Ms. Sudha Pillai, Member-Secretary
2. Shri Pronab Sen, Pr. Adviser
3. Shri Chaman Kumar, Addl. Secretary & FA
4. Shri C. Muralikrishna Kumar, Sr. Adviser
5. Shri T.K. Pandey, Joint Secretary (Admn.)

Unique Identification Authority of India (UIDAI)

1. Shri Nandan Nilekani, Chairman
2. Shri R.S. Sharma, Director-General

370 371

2. The Committee took evidence of the representatives of the Ministry of Planning and Unique Identification Authority of India (UIDAI) in connection with the examination of the National Identification Authority of India Bill, 2010. Major issues discussed with the representatives included, need for providing statutory status to the Unique Identification Authority of India (UIDAI); Definition of 'Resident'; provision for de-activating the Aadhaar Number; collection of demographic information and biometric information; nature of enrolment and special measures for enrolment of weaker sections. The Chairman directed the representatives to furnish replies to the points raised during the sitting within one week.

The witnesses then withdrew.

A verbatim record of proceedings was kept

The Committee then adjourned.

371
372

**MINUTES OF THE NINETEENTH SITTING OF THE STANDING COMMITTEE ON FINANCE
(2010-11)**

The Committee sat on Wednesday, the 29th June, 2011 from 1130 hrs to 1400 hrs.

PRESENT

Shri Bhartruhari Mahtab -- Acting Chairman

MEMBERS

LOK SABHA

- 2 Shri C.M. Chang
- 3 Shri Bhakta Charan Das
- 4 Shri Gurudas Dasgupta
- 5 Shri Nishikant Dubey
- 6 Shri Marigani Lal Mandal
- 7 Shri Magunta Sreenivasulu Reddy
- 8 Dr. Kavuru Sambasiva Rao
- 9 Shri Sarvey Sathyanarayana
- 10 Shri Dharam Singh

RAJYA SABHA

- 11 Shri S.S. Ahluwalia
- 12 Shri Raashid Alvi
- 13 Shri Moinul Hassan

SECRETARIAT

- | | | |
|------------------------------|---|---------------------|
| 1. Shri A. K. Singh | – | Joint Secretary |
| 2. Shri R.K. Jain | – | Director |
| 3. Shri T. G. Chandrasekhar | – | Additional Director |
| 4. Shri Kulmohan Singh Arora | – | Under Secretary |

Part I

(1130 hrs. to 1145 hrs.)

2. In the absence of the Chairman, the Committee chose Shri Bhartruhari Mahtab, M.P. to chair the sitting under Rule 258(3) of the Rules of Procedure.

- | | | | | |
|----|----|----|----|-----|
| 3. | XX | XX | XX | XX. |
| | XX | XX | XX | XX |

372
373

Part II

(1145 hrs. to 1215 hrs.)

WITNESSES

National Human Rights Commission (NHRC)

1. Shri Rajiv Sharma - Secretary-General
2. Shri A.K. Garg - Registrar (Law)
3. Shri J.P. Meena - Joint Secretary (P&A)

4. The Committee heard the representatives of the National Human Rights Commission on "The National Identification Authority of India Bill, 2010". The major issues discussed during the sitting broadly related to nature, objective and beneficiaries of aadhaar number; possible discrimination and specific provisions that are required to be built in; safeguards needed for securing the stored information by the proposed National identification Authority of India; implications of the provisions of the Bill on the individual's right to privacy, etc. The Chairman directed the representatives of the National Human Rights Commission to furnish replies to the points raised by the Members during the discussion within a week.

The witnesses then withdrew.

Part III

(1215 hrs. to 1300 hrs.)

WITNESSES

Indian Banks' Association (IBA)

1. Shri M.D. Mallya - Chairman
2. Dr. K. Ramakrishnan - Chief Executive
3. Shri M.R. Umarji - Chief Advisor-Legal

5. Subsequently, the Committee heard the representatives of the Indian Banks' Association (IBA) on "The National Identification Authority of India Bill, 2010". The major issues discussed during the sitting broadly related to stipulations prescribed by the Ministry of Finance and the Reserve Bank of India for using aadhaar numbers for opening bank accounts; new account holders added through aadhaar numbers; and utility of aadhaar number in

financial inclusion, social sector lending, etc. The Chairman directed the representatives of Indian Banks' Association (IBA) to furnish replies to the points raised by the Members during the discussion within a week.

The witnesses then withdrew.

Part IV

(1300 hrs. to 1400 hrs.)

WITNESS

Dr. Reetika Khera, Visitor, Centre for Development Economics, Delhi School of Economics

6. The Committee then heard Dr. Reetika Khera, on "The National Identification Authority of India Bill, 2010". The major issues discussed broadly related to nature of Aadhaar number; existing ID proof documents and need for aadhaar number, usage and benefits of aadhaar number particularly in Mahatama Gandhi National Rural Employment Guarantee Scheme, Public Distribution System, implications of the UID programme; relevance of Report of London School of Economics on UK's Identity Act 2006 in the context of aadhaar number etc. The Chairman directed the expert to furnish replies to the points raised by the Members during the discussion within a week.

A verbatim record of the proceedings was kept.

The witness then withdrew

The Committee then adjourned at 1400 hours.

375
374

MINUTES OF THE TWENTY-SECOND SITTING OF THE STANDING COMMITTEE ON FINANCE (2010-11)

The Committee sat on Friday, the 29th July, 2011 from 1100 hrs to 1715 hrs.

PRESENT

Shri Yashwanth Sinha -- Chairman

MEMBERS

LOK SABHA

2. Dr. Baliram (Lalgañj)
3. Shri C M. Chhang
4. Shri Gurudas Dasgupta
5. Shri Nishikant Dubey
6. Shri Bhartruhari Mahtab
7. Shri Mangani Lal Mandal
8. Dr. Kavuru Sambasiva Rao
9. Shri Manicka Tagore

RAJYA SABHA

10. Shri S.S. Ahluwalia
11. Shri Raashid Alvi
12. Shri Moinul Hassan
13. Shri Satish Chandra Misra
14. Shri Mahendra Mohan
15. Dr. Mahendra Prasad
16. Dr. K.V.P. Ramachandra Rao

SECRETARIAT

1. Shri A. K. Singh -- Joint Secretary
2. Shri R.K. Jain -- Director
3. Shri Ramkumar Suryanarayanan -- Deputy Secretary
4. Shri Kulmohan Singh Arora -- Under Secretary

Part I
(1100 hrs. to 1130 hrs.)

| | | | | |
|----|----|----|----|-----|
| 2. | XX | XX | XX | XX |
| . | XX | XX | XX | XX. |

Part II
(1130 hrs. to 1300 hrs.)

WITNESSES

| | | | | |
|----|----|----|----|-----|
| 3. | XX | XX | XX | XX. |
| . | XX | XX | XX | XX. |

The witnesses then withdrew.

375
376

Part III
(1400 hrs. to 1715 hrs.)

WITNESSES

Confederation of Indian Industry (CII)

1. Mr Arun Duggai
Vice Chairman, International Asset Reconstruction Company (IARC)
and Chairman Shriram Capital Limited
2. Mr Chirag Jain,
Chief Operating Officer
Canara HSBC Oriental Bank of Commerce Life Insurance Company Limited
3. Mr Ravi Gandhi,
VP, Corporate Regulatory Affairs
Bharti Airtel
4. Mr Rameesh Kailasam,
Program Director
IBM India Pvt. Limited

4. The Committee heard the representatives of Confederation of Indian Industry (CII) in connection with examination of 'The National Identification Authority of India Bill, 2010'. The major issues discussed included, existing ID proof documents and the rationale and necessity of aadhaar number, usage, benefits and objects of aadhaar number; role of aadhaar number in planning and formulation of social policies; collection of biometric and demographic information; measures for enrolment of certain categories like persons with disability; exploration of alternate and economical identity system; opening up of Registrars and enrolment agencies to private sector; technological issues involved in the UID project; financial implications of the UID project; impact of the provisions of the Bill on the individual's right to privacy; potential of possible use of aadhaar numbers by illegal residents; lessons learnt from global practice and failures experienced in different countries in establishment of identity system similar to aadhaar number especially relevance of report of London School of Economics on UK Identity Act, 2006; legality of implementation of the UID project before the law is enacted by the Parliament;

376 377
making the penal provisions of the Bill in line with IT Act, 2000 etc. The Chairman directed the representatives of Confederation of Indian Industry (CII) to give suggestions clause-by-clause along-with the replies to the points raised by the Members within ten days.

The witnesses then withdrew.

WITNESSES

Experts

1. Dr. Usha Ramanathan,
Independent Law Researcher on the jurisprudence on Law,
Poverty and Rights, New Delhi
2. Dr. R. Ramakumar,
Associate Professor,
Tata Institute of Social Sciences, Mumbai
3. Shri Gopal Krishna,
Member, Citizen Forum for Civil Liberties, New Delhi

5. The Committee then heard the experts on "The National Identification Authority of India Bill, 2010". The major issues discussed broadly related to beneficiaries of aadhaar number including the eligibility of children; feasibility study on the UID project; costs and benefits analysis of the UID project; global experience in creation of a national data base of its citizens with biometrics; convergence of data, its usage and its consequences; functioning of the UIDAI under Executive order and implementation of the UID project before an enactment of law; impact of the provisions of the Bill on civil rights and liberties; implications of the provisions of the Bill on RTI Act, 2005; responsibilities of 'Introducer' and liability of the UIDAI; outsourcing of works by the UIDAI and its responsibilities; alternate system of identification etc. The Chairman directed the experts to furnish replies to the points raised by the Members during the discussion within ten to fifteen days.

A verbatim record of the proceedings was kept.

The witnesses then withdrew

The Committee then adjourned

Minutes of the Sixth sitting of the Standing Committee on Finance (2011-12)

The Committee sat on Thursday, the 08th December, 2011 from 1500 hrs. to 1615 hrs.

PRESENT

Shri Yashwant Sinha – Chairman

MEMBERS

LOK SABHA

2. Shri Shivkumar Udasi Chanabasappa
3. Shri Harishchandra Deoram Chavan
4. Shri Bhakta Charan Das
5. Shri Nishikant Dubey
6. Shri Chandrakant Khaire
7. Shri Bhartuhari Mahtab
8. Shri Prem Das Rai
9. Dr. Kavuru Sambasiva Rao
10. Shri Rayapati S. Rao
11. Shri Magunta Sreenivasulu Reddy
12. Shri G. M. Siddeswara
13. Shri Yashvir Singh
14. Shri R. Thamaraiselvan
15. Dr. M. Thambidurai

RAJYA SABHA

16. Shri S.S. Ahluwalia
17. Shri Raashid Alvi
18. Shri Vijay Jawaharlal Darda
19. Shri Moinul Hassan
20. Shri Satish Chandra Misra
21. Shri Mahendra Mohan
22. Dr. Mahendra Prasad
23. Dr. K.V.P. Ramachandra Rao
24. Shri Yogendra P. Trivedi

SECRETARIAT

- | | | |
|---------------------------------|---|------------------|
| 1. Shri A. K. Singh | – | Joint Secretary |
| 2. Shri R.K. Jain | – | Director |
| 3. Shri Ramkumar Suryanarayanan | – | Deputy Secretary |

379
378

2. The Committee took up the following draft Reports for consideration and adoption:-

- (i) The Insurance Laws (Amendment) Bill, 2008;
- (ii) The National Identification Authority of India Bill, 2010; and
- (iii) The Banking Laws (Amendment) Bill, 2011.

3. The Committee adopted the above draft reports with some minor modifications/changes as suggested by Members. The Committee authorised the Chairman to finalise the Reports in the light of the modifications suggested and present these Reports to Parliament.

The Committee then adjourned

True Copy
SP
Ad ✓

Exh - 'N'

18/10/12

379

380

Bathinda UID agency may have violated norms in sensitive data collection

Nayjeevan Gopal : Bathinda, Fri Jun 24 2011, 03:29 hrs

Related Articles

- MMRDA hopes to acquire Aerial plot soon for Metro rail corridor
- DCP asks Punjab SHO to probe complaint
- UIDA's housing plot scheme likely to be delayed by 4 months
- Pink waste for elephants, cloth for Maya in Noida
- Firm denies wrongdoing, authority says need to examine whether violations have taken place

An empanelled enrolment agency of Unique Identification Authority of India may have violated the norms laid down by the authority and given collection of sensitive data from residents of Bathinda district to other firms

Sources alleged Alankit Finsec Ltd, which is the empanelled agency for the demographic and biometric data collection for the 12-digit unique number Aadhaar, had given the work for Bathinda district to a person named Nitin Singla, who in turn sub-contracted it to some other local people

As per the contract between Punjab Food and Civil Supplies Department, the registrar in the contract, and Alankit Finsec Ltd, the agency was to be paid Rs 30 per enrolment but sources alleged Alankit had outsourced it to Singla for Rs 14, who further sub-contracted it for cheaper rates to others

But Singla denied the allegation and claimed he worked as a area manager with Alankit Finsec Ltd. "I am an employee of Alankit Finsec Ltd and no work has been outsourced by the agency nor it has been outsourced to me by the agency," Singla claimed.

UIDAI pays Rs 50 to state government for every enrolment and leaves it to the state to decide on selecting the enrolment agency

UIDAI Deputy Director General (Establishment) D Kumar maintained that as per the norms no outsourcing can be allowed. "But whether any violation has taken place is to be first seen by the registrar (Punjab Food and Civil Supplies Department) and by our office in Chandigarh," he said.

Punjab Food and Civil Supplies Director Alk Nanda Dyal said she would examine the matter. "I would go through the guidelines and examine the matter," she said

UIDAI Assistant Director General in Chandigarh, Charu Bali, said, "I am not sure whether it is a violation or not. It is a policy matter and officials from head office can better speak on this. It is, however, not practically possible for the enrolment agency to have all the required manpower on the company rolls. There are certain liberties to enrolment agencies and to certain extent the agencies can outsource manpower"

However, the guidelines for selecting the enrolment agency in the Request for Quotation (RFQ) in the official website of UIDAI categorically states: "The supplier (read enrolment agency) shall not be permitted to sub-contract any part of its obligations, duties, or responsibilities under the contract."

In Belhara village, one Kunal Sharma, who claims to be a partner with Softel Systems, said they had been given the work to collect the data by Nitin Singla.

"We have been provided the equipment and are being paid Rs 9 per card for collecting the details," Sharma told The Indian Express

But Singla refuted Sharma's claims and said he was also an employee of Alankit. "Only he (Kunal Sharma) knows why he said so (that work was outsourced to Softel Systems for Rs 9 per card)," he said.

Alankit, on its part, has claimed that there was nothing wrong in outsourcing work. "We are operating in 10 states of India. We cannot hire operators and manpower for the company in the each and every part. There is no bar in outsourcing the job to arrange the manpower for us. The equipments for carrying the job have been provided by us. Moreover, the salaries to the manpower are being paid by us," Viney Chawla, company secretary of Alankit, said.

On whether the agency complied with guidelines related to labour laws, provident fund and minimum wages while utilising the services of such manpower, Chawla said, "It is the responsibility of the manpower provider."

Probe in Muktsar

Sources said following a complaint that "behaviour of operators was not resident friendly", the UIDAI has initiated a probe in Muktsar district. Sources alleged that the enrolment agency, which is collecting the demographic and biometric data of residents in Muktsar, is also an Alankit group company. "Yes, there is a complaint that residents are not able to talk to officials of enrolment agency in Muktsar and are not being guided properly. We are looking into the complaint," Bali said

EXH - C
16/10/12
38
380

DECEMBER 2, 2011

Cover Story

Why it failed in U.K.

Interview with Dr Edgar

BY R. RAMAKUMAR

"Biometric matching is not a perfect process. There is an element of judgment, and there will always be the result: 'This fingerprint is pretty close to three other fingerprints', which you then need to check manually and figure out."

DR EDGAR WHITLEY is Reader in Information Systems at the Information Systems and Innovation Group in the London School of Economics and Political Science. He has a PhD in Information Systems from the LSE. His research and practical interests include global outsourcing, social aspects of IT-based change, collaborative innovation in an outsourcing context, and the business implications of cloud computing. He is also an expert in identity, privacy and security issues relating to information- and Net-based technologies.

Whitley was the research coordinator of the LSE Identity Project and represented the project at the Science and Technology Select Committee review of the scheme. He has written extensively about the United Kingdom's identity cards programme for both academic and trade audiences and is a frequent media commentator on the scheme. His recent publications include work on the technological and political aspects of the programme. In 2009, he co-authored with Gus Hosein a book titled *Global Challenges for Identity Policies* (Palgrave Macmillan, Basingstoke, U.K.). He spoke to *Frontline* at his LSE office on October 18.

Thank you Edgar for agreeing to do this interview. You would have guessed that the decision to do this interview is inspired by certain recent events in India, where an identity project largely similar to the project in the United Kingdom is being implemented. In your view, what were the major



EDGAR WHITLEY: "THERE was the question of the scheme's legality."

reasons behind the U.K. government's decision in 2004 to bring in an identity card project? Was there only an "internal security" dimension to it? Or were there other dimensions, too, such as "developmental"?

In many ways, this is a really great question to begin the interview, because it is kind of a puzzle that we have never been able to find a satisfactory answer to ourselves. The idea of having identity cards has been one that almost every Home Secretary had at least thought about and had some consultations with civil servants at some stage, before they backed out. So, in the U.K., in 2002, there was a discussion about "entitlement cards" that slowly gave way to "identity cards". I think the idea that there was a single policy reason or a few policy reasons behind the identity card project would not fit the facts well. If you take

entitlements to access public services, then a few features of the project could be thought of as leading us to such a view. If you take national security, then, certain other features of the project could be thought of as leading us to such a view. In addition, there was a real space where I could have jokingly said about the reasons behind the project as, "Oh, it is Tuesday today, so for today 'X' might be the reason behind the project." This was partly the way the description, discussion and arguments for the project evolved over time, both naturally as a policy development and in response to the challenges and questions that the project faced at each point of time.

So, by about 2009, when the popularity of the project was faltering badly, to put it mildly, emphasis suddenly moved to enabling young people, who did not necessarily have a detailed credit history or biographical footprints, to be able to prove who they are for frequent transactions, such as opening a bank account or registering for a mobile phone number, and so on. This particular strategy was a response to the fact that other claims were not proving to be successful, as they had initially hoped. Another argument was that this scheme would help to build confidence in people working in airports, which was a typical "national security" reason. But the airport unions fought back against it and they had to limit it to two small trial projects in two small airports. During other times, some of the arguments put forward were responses to policy design decisions. So, sometimes they thought it may be better to emphasise the idea that the ID card can be used to travel freely across Europe without carrying passports.

So, the claims and responses kept changing. That is why I said it was a great question to begin this conversation. If the idea of having a centralised database was to address questions of identity fraud, so that people would not have more than one identity card, then there were other ways in which you could do that without resort to such centralisation of personal infor-

"Evidence showed that such schemes performed best when set up for clear, focussed purposes."

mation. So, I suspect there was a broad kind of direction; when some aspects of the project appeared to be faltering in popularity, other claims were made, and this process continued as the project evolved.

DISCRIMINATION CONCERNS

Was the "entitlement card", linked to the ID card project, linked to reforms in the National Health Services (NHS), that is, to reduce leakages?

It was essentially about concerns about people who were not entitled to public-funded services like the NHS having access to them. So, if students were entitled to the NHS during the period of their study, and they didn't return to their home country, maybe you could argue that fraud could be reduced if you insist that the ID card should be produced at the NHS centres. But there are practical problems that emerge from this policy. The counter argument was that this makes the doctor a receptionist, equates him to a border official, having to do duties way beyond what he was reasonably expected to do. Further, this also rewrites what citizenship or entitlement actually means.

There is also a very practical risk of discrimination. If a surgeon is doing this checking for entitlement, and I, as a white middle-class male, come along and say, "I am sorry, I don't have my card with me, but I would like to book a doctor's appointment", will I be treated in the same way as a U.K. national whose skin colour is not white and first

language is not English? The latter might be checked more despite the fact that their entitlement is exactly the same as mine, and there are consequential concerns of discrimination that are very serious.

What were the major arguments in the LSE report?

We had argued that the ID card system could offer some basic public interest and commercial sector benefits. But we also identified six key areas of concern with the government's plans. First, evidence from other national identity systems showed that such schemes performed best when established for clear and focussed purposes. The U.K. scheme had multiple, rather general, rationales, suggesting that it had been 'gold-plated' to justify the high-tech scheme.

Secondly, there was concern over whether the technology would work. No scheme on this scale had been undertaken anywhere in the world. The India project is, of course, even bigger. Smaller and less ambitious schemes had encountered substantial technological and operational problems, which may get amplified in a large-scale national system. The use of biometrics created particular concerns, because this technology had never been used on such a scale.

Thirdly, there was the question of the scheme's legality. A number of elements of the scheme potentially compromised Article 8 (privacy) and Article 14 (discrimination) of the European Convention on Human Rights. The government was also in breach of law by requiring fingerprints as a prerequisite for receipt of a passport. There was a lot of talk from the proponents about international obligations. However, the report found no case as to why the ID card requirements should be bound to passport documents.

Fourthly, we felt that the National Data Register was likely to create a very large data pool in one place that could be an enhanced security risk in case of unauthorised accesses, hacking or malfunctions.

Fifthly, according to us, an identity system that is well accepted by citizens is likely to be far more successful in use than one that is controversial or raises privacy concerns. This was important in order to realise the public value that citizens would want to carry their ID cards with them and to use them in a wide range of settings.

Finally, the cost part. Compliance with the ID cards Bill would have meant that even small firms would have had to pay £250 for smartcard readers and other requirements, which would have added to the administrative burdens that firms faced.

You have argued in the report that the "scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals". Was privacy the legal right you were referring to?

Yes, privacy in terms of the data controlled by the government. There was a separate concern about the audit trail. So, when you entered into a transaction where you had to produce your ID card, the design of the system was such that a record would be kept of every such verification. Good idea, because it allows you to check for forgery in transactions. However, the negative version of that is it provides a detailed record of every transaction you have done, which can be of interest to either people browsing the database or to security services or whoever. The record here wouldn't be just that your identity was verified; there would be a little more data associated with the transaction. For example, you went to Health Clinic Number 45. They used your card and your fingerprint there for verification. They did this at 12:37 hours. There is a series of metadata associated with that visit that would be there in the audit trail. And, of course, it wouldn't take very long to realise that, actually, Health Clinic Number 45 is a sexual health clinic. If the audit trail also shows that you were there on a number of occasions, it might be reasonable to infer certain kinds of things that you perhaps do not want to disclose. Some things are not necessary to

"Government was in breach of the law by requiring fingerprints for receipt of a passport."

be disclosed, but which are being recorded and stored in an accessible way to various people because of the way the system is designed.

A second concern was with the way biometrics was being used. Although fingerprints and iris scans are useful ways of linking a person to their biometric, one problem if you take straightforward images is that they aren't revocable. So, if you have a password for your e-mail account, and you realise that someone has broken into your e-mail account, you can always reset your password. If the biometric is stolen, the possibility of revoking it becomes almost impossible. It's gone.

"Death of privacy' is what some argue in the wake of the massive technological advances that we have had. Your comments.

That is just one way of looking at the technological advances. To my mind, it is an overly deterministic proposition. What you are doing here is not allowing for user choice of designs and not allowing for innovative alternative designs. It's a too straightforward view. Clearly, there are privacy concerns that are more difficult to address with the new technologies. The fact that when you visit a web page, they know where you came from, what your browser configuration is, what plug-ins you have, what screen resolution, and so on. You could be pretty uniquely identified just from the browser. But there are things that you can do. You can do private browsing, you can have do-not-track options, you

can delete your cookies and if you are really sophisticated, you could also do things like onion routing. There are also opportunities for companies to declare themselves as privacy-friendly, and they could be good competitors to other companies that are not so privacy-friendly. So, the idea of "death of privacy" is too simplistic a view.

There are always alternatives; there are always different ways in which a society can respond to these kinds of concerns and issues. There are always possibilities to have privacy-enhancing means of identification. For instance, you could have an ID card with a chip, which has your fingerprint, or a part of it, stored as a template. It is not stored in any central database, but it is in the chip of your card and your card is with you.

So, when you have to prove that you are you, you could just swipe the card and give your fingerprint, after which you could be identified as the bearer of that card. No one gets your information stored in that card. That's a privacy-friendly way of identification.

The first generation technology here are chip cards, the second generation technology is stickers on your mobile phones and the third generation technology is a chip inside your mobile phone. The chip may have your name, your database, your fingerprint template and a little bit more data on who issued it and all that. But nothing about where you have been, no audit trails, no records and thus, privacy-enhancing.

Are there countries that have tried these methods?

This has not yet become the obvious way to do it because it takes a while to get your head around. The point here is that you need to understand what it is that you want. Technically, you only want proof that the person is himself and a little bit more.

BIOMETRIC MATCHING

You were very critical of the technology of biometrics being used

383

384

Cover Story

DECEMBER 2, 2011

in the project. You argued that "the technology envisioned for this scheme is, to a large extent, untested and unreliable". Was this assessment based on technical inputs from biometric experts? Could you elaborate on the comments from biometric experts?

We used some feedback from biometric experts, but we also independently looked at already published research work on biometrics. Certainly, in terms of the untestedness, the scales of studies that had been done for both fingerprints and iris scans were fairly limited.

There were far better performance results on a 1:1 match. So, this is Edgar's fingerprint on the database, here is Edgar, we do 1:1 match; this is more likely to work. But that was not how the U.K. was planning to use it. The U.K. was trying to use biometrics to also prevent duplicate identities. The idea was that even if I try to enrol twice, and even if I had created a fake biographic identity (say, a John Smith with a different address), when my fingerprint came in for a second time, the system should come along and say: "We know this fingerprint, and this belongs to Edgar Whitley" and not say, John Smith. Here you have a match every single biometric with every single previous biometric.

Biometric matching is not a perfect process. There is an element of judgment, and there will always be the result: "This fingerprint is pretty close to three other fingerprints", which you then need to check manually and figure out. But this increases the cost, let alone concerns about reliability.

Now, there is always a possibility of a fraudulent use; that is, if I am really John Smith, I could have applied with Edgar Whitley's biographical details. That's possible, though difficult.

So, for instance, victims of domestic abuse could be given a completely new identity with a stolen set of biometrics.

You also have major issues with gender reassignment, which will create unnecessary interferences into your private life.

The U.K. project was to have iris scans, but they were dropped later. Was there a reason?

Iris scans were always present in the documents that were discussed in Parliament. The proponents of iris scans claim that they are far better than fingerprints at differentiating people. That is because you collect a far larger number of data points in your iris scan than in the fingerprint. The problem with the iris biometric at that time was that the set-up for the capture of the iris biometric had to be well managed.

"You could have an ID card with a chip, which has your fingerprint, or a part of it, stored as a template."

If there is a sudden good sunshine, very noticeably the room is brightened up. So, you need to potentially adjust your iris-capture device to allow for those kinds of set-ups. But we know from the experience of airports that iris devices often have problems in operating at their full performance level; airports are designed by architects, and architects use lots of glass and open space, which allow for light to come in seamlessly and brighten up the space. This creates a lot of problems for iris recognition systems.

There is also interesting empirical research that shows that as you move from one version of the technology to newer versions, you get performance differences because they capture iris images slightly differently.

So, you don't get quite the same results in matching as you move with versions. These were the reasons why the U.K. government dropped iris scans from the plan in 2006.

What was the nature of the response among the British people to the identity project? Were there mass protests? Or was it mostly through the social media that the protest spread? And, was it due to these protests that the project was finally shelved in 2010?

It got scrapped because the parties that came to power were opposed to it. In practice, you don't vote on the basis of your view of one single scheme. There was a lobby group called "NO2ID", which was very effective in getting the message out about their concerns with the whole process. I was on their mailing list, and every week, along with the news items on the scheme, there was also information on where meetings were to be held, where you could meet MPs and ask questions about the scheme, and so on. Scores of local activists got involved in this, again from both the Left and the Right. This was no civil disobedience movement, but just explaining what these proposals were and what they are going to mean, and trying to convince people over what some of the dangers were.

They were also continuously talking to journalists and explaining what this meant in practice, at levels of detail. They kept telling journalists why biometrics could not be the "magic bullet". The press coverage was overwhelmingly comfortable with that critical analysis.

The technology press and its science and technology correspondents were eager to deal with these questions. They asked those questions. So, there was general awareness building in a major way.

Have you been following the Indian debate around unique ID numbers? Any views?

I have been following it one step removed. We have been speaking to people though. I think in India, too, it is important to raise these policy questions that I referred to just a while back.

Thank you very much, Edgar. ☐

True copy
52

The UID Project and Welfare Schemes

REETIKA KHEIRA

This article documents and then examines the various benefits that it is claimed, will flow from linking the Unique Identity number with the public distribution system and the National Rural Employment Guarantee Scheme. It filters the unfounded claims, which arise from a poor understanding of how the PDS and NREGS function, from the genuine ones. On the latter, there are several demanding conditions that need to be met in order to reap marginal benefits. A hasty linking of the PDS/NREGA with the UID can be very disruptive. Therefore, other cheaper technological innovations currently in use in some parts of the country to fix existing loopholes in a less disruptive manner are explored.

I would like to thank Jean Drèze, Alok Shukla and Kamal Mali for discussions on some of these issues

Reetika Kheira (reetika.kheira@gmail.com) teaches at the Indian Institute of Technology, Delhi

The Unique Identification (UID) project is a flagship project of the United Progressive Alliance-II (UPA-II) government. The Unique Identification Authority of India's (UIDAI) ambitious plan of issuing a unique biometric-enabled number, innocuously called "Aadhaar", to every Indian resident has also begun to generate a debate on citizen-state relations, privacy, financial implications, and operational practicalities.¹

What the debate has largely missed so far, however, is the credibility of the UIDAI's claims in the field of social policy, particularly the National Rural Employment Guarantee Act (NREGA) and public distribution system (PDS). A number of claims ("the project possesses the power to eliminate financial exclusion, enhance accessibility, and uplift living standards for the majority poor") have been made by the UIDAI, but have not been carefully analysed.

In this article, I filter the unfounded claims from the valid ones. The misleading claims with respect to the NREGA and PDS seem to be the result of superficial research into what ails these two programmes. Even with respect to the valid claims, such as helping with de-duplication of PDS cards, there are caveats which have not been adequately discussed so far.

Thus in Sections 1 and 2, the focus is on what the UID can and cannot do for the NREGA and PDS. In the next section, the possible fallout of a hasty imposition of UID on the NREGA/PDS is examined briefly. I also examine the scenario in which the existence of the "soft infrastructure" that the UIDAI aims to provide is important – namely, a transition from NREGA and PDS to cash transfers. The government needs to initiate an open discussion on cash transfers (if they are on the cards) rather than attempting to make a surreptitious transition to them. In the final section, I highlight some of the larger concerns

related to a project such as the UID, by drawing a few parallels between the now-abandoned United Kingdom Identity Bill and the UID project in India.

Before proceeding, it is worth recalling that being enrolled in the Aadhaar database and being given a number in itself carries no welfare benefits. Having an Aadhaar number does not eliminate the need to apply for a bank account, or a ration card or a job card (required to be eligible for work under NREGA). It can only serve as a valid form of identity in the same way that a driver's licence or passport currently do.

1 NREGA: Barking Up the Wrong Tree?

The UIDAI has a four-page document on NREGA. From this document, it is clear that its officials are poorly informed on issues relating to NREGA. Resulting from its poor understanding of the programme are several claims of improving efficiency in government spending. I discuss a few of these claims below: controlling corruption in NREGA, eliminating financial exclusion, preventing exclusion from government programmes due to the lack of identity proof, and so on.

One good example of the UIDAI being poorly informed is its statement regarding NREGA wage payments (Government of India 2010a: 2). The UIDAI claims that the UID will enable financial inclusion, but it seems to be unaware that wage payments through banks and post offices became mandatory in 2008. The transition to bank payments is now largely complete. A large majority of NREGA workers already have a bank (or post office) account: more than nine crore NREGA accounts (covering 83% of NREGA job cards) were opened by the end of 2009-10. This is not to say that the opening of bank accounts was a smooth process. The main hurdle was not so much the Know Your Customer (KYC) norms (as claimed by the UIDAI) but that the coverage of banks and post offices in rural areas is inadequate, the ones that exist are under-staffed, and post offices in many parts do not maintain computerised records.² Tamil Nadu is the only state that still makes cash payments, on the grounds

385
386

that it is able to control leakages within the cash system and that cash payments help to ensure timely disbursement of wages. Field evidence suggests that there is some truth in this claim of the Tamil Nadu government (Khera and Muthiah 2010).

The claim of controlling corruption through the UID is made on the premise that payments are still being made in cash. In the days of cash payments of NREGA wages, the main source of embezzlement was by fudging attendance records – by either adding names of people who had not worked, or inflating the attendance of those who had worked. Payment of wages through banks and post office has made wage corruption quite difficult. However, three potential channels for siphoning off money remain open – extortion, collusion and deception.⁴ Extortion means that when “inflated” wages are withdrawn by the labourer, the middleman turns extortionist and takes his share from him or her. Collusion means that the labourer and the middleman agree to share the inflated wages that are credited to the labourer’s account. Deception means that middlemen open and operate accounts on behalf of labourers, withdraw the inflated wages from these bank accounts, pay workers their due in cash, and pocket the difference. Biometric-enabled UID to authenticate identity can help to prevent “deception”, but is of little use in preventing collusion or extortion.

Facilitating “doorstep banking” through banking correspondents (the “BC model”) is supposed to be another benefit of the UID. At the moment, labourers often have to go long distances to withdraw their wages. Banking correspondents (intermediaries who extend banking services to remote villages) are supposed to enable disbursement of wages at their doorstep. Here again, however, there are issues of practicality and effectiveness, and we need to consider alternatives. Modernising and computerising post offices would also contribute to making banking services accessible. As a long-term measure, the government should consider an expansion of the rural banking network. Appointment of local kirana stores as banking correspondents could be a regressive step, as it would mean routing NREGA wages through the local bania (often a moneylender also).

The BC model could end up diluting the sanctity of existing banking practices.

At the end of the day, it is not clear from the UIDAI documents exactly how UID is supposed to help NREGA. There is no obvious problem of “identity fraud” in NREGA that UID is waiting to resolve. There is no evidence, for instance, of fake job cards being a major problem. An NREGA job card is not like a ration card, which automatically entitles the holder to subsidised grain. To get benefits under the NREGA, the job cardholder is required to work – so a fake job card is of little use *per se*. Claiming benefits without working requires collusion between non-working job cardholders and implementing officials. If the two parties collude, some job cardholders can have wages credited to their bank accounts, by getting on muster rolls. UID purports to prevent this through “biometric attendance at the worksite”, but the practicality of this imaginative idea is far from clear – it could easily create more problems than it resolves. And some forms of collusion can persist even with biometric attendance at the worksite.

For the NREGA, the UID, if it works, will help to plug some minor loopholes. This does not justify the sweeping claims that are made. In Section 3, I discuss the disruption that it can cause, if the UID and NREGA are linked.

2. PDS: Is There a Case for the UID?

2.1 Improving Inclusion

Similar claims are made with respect to the PDS. For instance, the UIDAI often claims that the project will improve access to government services. UIDAI officials have said that many Indians are deprived of government benefits because they do not have the required identity proof.⁵ This claim is based on an incorrect diagnosis of why people are excluded from government schemes.

There are two important causes for the exclusion of a large number of people from government programmes – one, poor coverage related to low allocations for these programmes and two, misclassification of people. Social welfare expenditure in the country is not adequate to provide universal benefits (Gupta 2010). In such a situation, the government has

resorted to making many social welfare schemes targeted programmes. When schemes are targeted, benefits are conditional upon being classified, say, as a below poverty line (BPL) family. The selection of BPL families is based on a census which is conceptually flawed and poorly implemented (Hirway 2003, Swaminathan and Mishra 2001, Khera 2008, Drèze and Khera 2010a).

Note that misclassification of families in the “BPL census” has little to do with identity fraud or “duplication”. Misclassification can occur when the criteria used for identification of BPL families are incorrect (e.g. in a previous BPL census, the ownership of a fan led to exclusion of families from the BPL list) or when government criteria are not adhered to (e.g. families misreport their status, or the surveyor records incorrectly).

Yet the UIDAI gives the impression that misclassification of households can be controlled (if not stopped) with the help of unique identity numbers. “The eventual nature of an Aadhaar-linked approach in PDS would depend on the particular benefits the government hopes to gain. Using Aadhaar solely for identification would enable *clear targeting of PDS beneficiaries*, the inclusion of marginal groups, and expanded coverage of the poor through the elimination of fakes and duplicates” (Government of India 2010b, 3, italics added).

2.2 Portability of Benefits

The UIDAI also makes a claim of “portability of benefits”, i.e. that with a UID, beneficiaries can claim their benefits wherever they are. A PDS that allows beneficiaries to draw their rations from anywhere in the country would indeed be a desirable improvement over the present system. The portability argument is perhaps the most enticing aspect of the UID programme. However, this too is not very well thought through. Though the UID is portable, benefits may not be, because the latter present operational issues that cannot be solved by the UID. The possibility of making the current form of identity authentication (i.e. the ration card) “mobile” has not been explored. A computerised database of cardholders, with holograms and/or barcodes on ration cards, could also make ration cards mobile. Smart cards or food

PERSPECTIVES

coupon: can also serve the purpose of providing a portable identity, which can be easily authenticated anywhere.

Returning to operational issues related to portability, if benefits are portable and grain allocations to PDS outlets are based on the previous month's sales (as recommended by the UIDAI), matching supplies to an unpredictable demand becomes difficult. If a state gets a fixed quantity of foodgrains, based on the number of ration cards from the central government, streamlining supply to cater to a PDS that allows portability of benefits is not a simple matter. Building in portability across states is especially challenging (think of interstate migration).⁷

2.3 Bogus Cards and 'De-duplication'

Another inflated claim relates to the elimination of "bogus" cards in the PDS. There can be three types of bogus cards: (a) "ghost" cards, i.e., where cards exist in the names of non-existent or deceased persons; (b) "duplicates" where one person or household, entitled to one card, manages to get more through unfair means; and (c) "misclassified" cards, when ineligible persons/households claim benefits (or, inclusion errors).

The main fallout of "bogus" cards where schemes are targeted (such as the PDS) is that it denies a genuine beneficiary his/her entitlements. Elimination of bogus cards can contribute to improving the efficiency of government schemes. The UIDAI can help eliminate only the first two types of bogus cards. As discussed earlier, UIDAI can do nothing about inclusion errors.

The question then arises, what proportion of all cards is bogus?⁸ Reliable data on the overall proportion of bogus cards are hard to find. Yet the UIDAI claims that ghost ration cards are the main problem: 'a key source of leakage identified in the PDS is subsidised food drawn from the ration shop in the names of eligible families by someone else' (Government of India 2010b: 8). Rough estimates based on newspaper reports (admittedly not the most reliable source for such data) put the proportion of fake cards in the 2-13% range (Chang 2010, IANS 2010 and Radhakrishnan 2010). In Tamil Nadu, only 2% of cards were bogus (Planning Commission 2004).

Bogus cards are indeed part of the problem, but there is not enough evidence to say that this is the main source of diversion from the PDS. This is one source of corruption, though quite likely it is not the largest source of diversion of PDS grain today (see more on this below).

Second, elimination of "ghost" and "duplicates" by biometric-enabled de-duplication requires that the Aadhaar number be compulsory (at least for that particular programme). This is best explained by Nandan Nilekani, the chairperson of UIDAI himself. "You can't make it mandatory in the first instance. Let's say a particular state decides to issue fresh ration cards from 1 May 2011. Now, they may decide to have Aadhaar numbers on all these cards. For some time, in parallel there will be the earlier cardholders who will not have Aadhaar. We can't completely eliminate duplication. But over time, as Aadhaar numbers in ration cards become nearly universal, they can then say 'from now onwards, only Aadhaar-based ration cards will be accepted'. At which point, duplication will cease to exist" (Sebastian 2010). The UIDAI will not make it compulsory to get an Aadhaar number. However, that does not stop them from encouraging various government departments to make it compulsory. There is a tension between voluntary enrolment and achieving de-duplication. Some of the implications are discussed in Section 3.

In Chhattisgarh, de-duplication has been attempted by computerising the database of ration cardholders and distributing new ration cards with holograms which make each ration card unique. The other option is the use of biometrics (say, at the stage of issuing ration cards), which the UIDAI proposes to use. Tamil Nadu keeps constant vigil on the number of ration cards to eliminate bogus cards.

2.4 The Last Mile Problem

A major cause of diversion from the PDS is the lack of a functional system of "last mile" authentication. In the current system, the movement of foodgrain is tracked till it leaves the godown for a ration shop.⁹ Ration dealers maintain a sales register and a monthly stock register, based upon which the next month's rations are supposed to be released. However, this

monthly squaring of records is operational only in a handful of states (including Chhattisgarh, Himachal Pradesh and Tamil Nadu). In other states, dealers fudge information in these registers.

This allows dealers to divert grain in two ways: first, cheating cardholders by underselling (e.g., he provides only 25 kg out of the 35 kg entitlement of a family) and yet make them sign for their full quota. When villagers are disempowered and forced to buy from the same dealer, with few options of being heard by higher authorities, they feel resigned to accept this smaller quantity. Second, illegal sale of PDS grain in the open market, en route to the village ration shop. Dealers then appear helpless in the village saying that they have been given less by the authorities (*pichhe se kam aya hai*).

There are several options to fix the "last mile" problem. Introducing food coupons for all entitled households is one way of dealing with this problem. In this coupon system, each household is required to deposit their coupon at the time of purchase. Dealers have to deposit these in order to get more grain released for the next month. The release of grain is tied to the number of coupons deposited back. Swiping smart cards or authenticating biometric information, at the time of purchase, can perform the same function.¹⁰ Even social audits (e.g., reading out details from the daily sales register maintained by the ration dealer) can be employed to resolve last mile issues. Other cost-effective and technology savvy solutions have been employed elsewhere – e.g., in Chhattisgarh grain is delivered to the village (in easily identifiable yellow trucks), so that a dealer cannot pretend that he did not get the grain; further, when trucks leave the godowns, an SMS alert is sent to a few persons in the village (Drèze and Khera 2010b). The real problem, then, is not so much the lack of options for last mile authentication. Rather it is the lack of political will to crackdown on the corrupt. Political will has been lacking because often politicians are part of the corrupt nexus.

Compulsory biometric authentication (with or without UIDAI) at the last mile would require us to consider cases of old or disabled or ill persons, who currently rely on neighbours or relatives to bring home

387
388

their ration. With biometric authentication there may not be any scope of buying their rations in the proposed new system. Quite likely, the UIDAI's response would be to say that an "over-ride" facility can be built into the system for such cases. But is this really practical (e.g., if a healthy person falls ill, how quickly can the system respond to his need for the override facility) and will it not again open the door to manipulation?

Before moving to the next section, note that for de-duplication and last-mile authentication, UID is one of at least three distinct options: smart cards, biometric, and the UID. The UID needs biometrics, not the other way round. The UIDAI does not make a clear distinction between the three, thus suggesting that they are the same. The relative merits and demerits – cost, technological requirements, possibility of fraud, etc. – of each of these options need serious consideration. One can have biometric authentication without building an integrated database as proposed by the UIDAI. The main utility of the integrated database envisaged by the UIDAI is that it would obviate the need for scheme-by-scheme enrolment which can be expensive.¹¹ But how many schemes of the Government of India need biometrics for purposes of de-duplication and solving the "last mile" problem? In the NREGA, as explained above, neither bogus cards nor last mile authentication are major concerns.

3 Implications for PDS and NREGA

As noted above, de-duplication can be achieved only by making enrolment compulsory (at least for particular schemes). The UIDAI has set itself a target of covering only half of India's population in the next four years. The UIDAI is engaging many registrars to meet its targets. In its eagerness to de-duplicate, there is a danger that the UID will be made compulsory in a rushed manner. Even with an ambitious target, the project will then end up excluding large sections of India's population.

Hasty integration of UID with the PDS or NREGA could, in practice, go against the rhetoric on "inclusivity". In fact, a "re-engineering" of the NREGA is currently underway.¹² This involves the engagement of "service providers" who will be responsible for enrolling individuals for UID, and

at a later stage, involved in authentication (including at the worksite using hand-held devices) of workers.

The consequences of this sort of re-engineering are likely to be disastrous for the NREGA. Job cards issued in 2006 are due to expire next year. If, for example, the Ministry of Rural Development links the provision of new job cards to getting a UID, many workers are likely to be denied work for sometime to come.¹³ There is a real danger that those who do not enrol will be turned away from the NREGA. We have already learnt this lesson – the hard way – when the transition to bank payments was made. Poorly equipped and understaffed banks and post offices were expected to open millions of NREGA accounts overnight. Those workers who did not have accounts began to be denied work.

Moving on to the PDS, one of the proposals mooted by the UIDAI is that PDS dealers buy their grain from the open market at the market price but supply it to PDS beneficiaries at a subsidised price fixed by the government. When a beneficiary buys his/her ration, she/he would be required to give the UID number and be authenticated biometrically. Once this is done, the dealer would be reimbursed the difference between the market price and the subsidised price with a small commission (Government of India 2010b: pp 45 and p 13). It is expected that since the difference between the market price and the sale price is reimbursed only when the dealer sells to the intended beneficiary, it will ensure that the dealer does not sell on the black market.

Interestingly, the origin of this new model for the PDS can be traced to a study commissioned by the India office of the World Bank (Ahasan et al 2008). The consultants (from a software vending company called Cal2Cal) prepared a report where the use of smart cards and biometrics as well as purchase of grain from the market was proposed (Cal2Cal 2008). This proposal was modified slightly by the Planning Commission – instead of dealers buying from the open market at market price, in the Planning Commission proposal the dealers are to be supplied by the Food Corporation of India.¹⁴

Such a proposal, involving a major overhaul of the current system, would

need to be discussed and tested on a pilot basis. Possible abuse needs to be explored and debated in a transparent manner. For instance, informal field visits to Chandigarh to study smart cards revealed that dealers keep the swiping machine inside the shop, and buyers have no way of verifying what is being punched into the machine. This suggests that even the smart card requires adequate safeguards (e.g., using automated receipts, voice-overs, etc.) against "deception". In some circumstances smart cards could even facilitate fraud, e.g. because people do not understand the whole technology (unlike entries in ration cards).

If the benefits of the UID project to two major existing social welfare programmes (NREGA and PDS) are marginal and uncertain, why is the government rushing ahead with it? In fact, the UID project with biometric authentication is very well suited for a particular type of welfare scheme, namely, cash transfers. Nandan Nilekani's *Imagining India* refers to such a proposal. "A smart-enabled, accessible national ID system would be nothing less than revolutionary in how we distribute state benefits and welfare handouts" (Nilekani 2008: 372). "The state could instead transfer benefits directly in the form of cash to bank accounts of eligible citizens, based on their income returns or assets" (ibid: 374). Planning Commission documents have also floated this idea.¹⁵ Cash transfers as a welfare measure are very different from both the NREGA and PDS. If it is the intention of the government to transition to cash transfers, then the government must be transparent about this proposal and allow a public discussion of it.¹⁶

4 LSE Identity Project Report

A project such as the UID raises a range of concerns.¹⁷ Though these are not the subject of this article, it is worth flagging these issues for the interested reader. These concerns have been comprehensively documented by the London School of Economics and Political Science Identity Project report (Henceforth LSE 2005). Though not entirely comparable, there are several parallels between the UK Identity Bill and UIDAI.¹⁸

First, the now-scrapped UK Identity Bill (UK-ID) was envisioned as a project for "combating terrorism, reducing crime and

illegal working, reducing fraud and strengthening national security".¹⁹ The UID project also has its origins in a national security project (as admitted by the chairman of the UIDAI himself).²⁰ Since the formation of the UIDAI, it has been projected as an initiative to promote social inclusion.²¹

Second, in both cases there seems to have been a tendency to make unfounded claims. For instance, as discussed earlier, the UIDAI claims that millions of Indians are without any identity which is the cause of them being excluded from the government's schemes. In the case of the UK-ID, the LSE (2005) report states "Many of the claims made about the prevalence of identity fraud are without foundation" (p. 9). Similarly, in both countries, the concerned authorities seem to have overplayed the incidence of "identity fraud" (or, in the Indian context and UIDAI's jargon, the need for 'de-duplication') in the social sector.²²

Third, both projects have raised legal concerns, e.g., the LSE (2005) report brought up the question of compromise or conflict with other laws (Disability Discrimination Act, Race Relations Act, Data Protection Act to name a few). Further, the report states "The legislation places requirements on individuals and organisations that are substantial and wide-ranging, and yet no indication has been given relating to how liability would be established, who would assess that liability, or who would police it" (LSE 2005: 13). On the other hand, the draft NIDAI Bill (which was placed on the UIDAI's website) had similar clauses, whereby individuals had responsibilities but with little obligation on the authority.²³ On the question of oversight too there are similar concerns in both projects (LSE 2005: 13, Drèze 2010 and Krishnaswamy 2010).

Fourth, the LSE (2005) report questions the project on technological (especially related to the scale of the project) and financial grounds. The LSE (2005) report is also quite circumspect on the question of biometrics (pp. 169-86). Two other reports suggest that the science of biometrics is not quite as exact as is commonly believed.²⁴ These reports further question the scalability of such an exercise.²⁵

Finally, and most surprisingly, in India no serious discussion of the cost of the UID project has taken place. Despite several

demands for a cost-benefit analysis, there is no such report so far. Interestingly, one of the main justifications for scrapping the identity project in the UK was its cost.

Concluding Remarks

The UID is projected as a "revolutionary" initiative, with unprecedented gains in efficiency and transparency. In this paper, I argued that several claims are unfounded or exaggerated and reflect a superficial understanding of the problems afflicting the implementation of NREGA and the PDS. As discussed earlier, there is little that the UID can do to improve implementation of NREGA. In the PDS, there are two problems to which the UID can contribute: last mile authentication and elimination of bogus cards.

An important caveat to bear in mind is that the UID can contribute to but is not necessary for, resolving these problems. The UID is one of several technological innovations that is possible. What is not mentioned in the UIDAI's documents is that many of the proposed technological inputs can be implemented *without* a costly UID. Other options are available (e.g., the use of food coupons or smart cards for last mile authentication). These options may well be cheaper, less disruptive, and more people-friendly (e.g., easier to understand), and have the additional advantage of having been tested on some scale in some parts of the country. The tendency to conflate all technology measures with UID creates the impression that it is a necessary condition for reform.

Needless to say, technology can contribute to improving the efficiency of these programmes, and is often welcome. Examples of cost-effective technology that enhances transparency and empowers people are readily available – e.g., computerisation of PDS operations in Chhattisgarh and Tamil Nadu, SMS-based alert systems, and so on. Further, other measures for transparency cannot be discounted simply because they do not involve technological inputs. For instance, in Rajasthan, 'transparency walls' listing all job cards issued, along with days of employment in a particular financial year allow people to monitor NREGA expenditure just as much as the on-line MIS. However, even technology has its limits. One issue related to this that has not been discussed adequately is

the feasibility of maintaining an updated database of close to one billion people.

Finally, the possible disruption that the transition to a UID-enabled system can cause must be faced squarely by the government. The UID's contribution to plugging leakages is likely to be marginal in the case of the PDS, and even less in NREGA. However, these marginal benefits can be realised only by making a wholesale migration to a new, complex and untested system. In the process, there is a real danger that the UID will end up hurting the very people it seeks to help.

It is time to go beyond the hyped benefits of UID and to recognise that, if it succeeds, the benefits in NREGA and PDS will be quite modest. If the UID project is to pave the way for cash transfers, the government needs to state this upfront and allow public debate on the issue.

NOTES

1. On these issues see Debrzy (2010), Drèze (2010), Gupta (2010), Maranganji (2009), Ramanathan (2010a, 2010b and 2010c), Ramkumar (2010), Sharma (2010), and Shukla (2010).
2. This part of the paper elaborates the discussion in an earlier article. See Khosla (2010).
3. See Adhikari and Bhattacharya (2009) for details on the problems, advantages and labourers' perceptions of the transition to bank/post office payments.
4. On the issue of corruption and the transition to bank and post office payment of NREGA wages, see Siddharth and Vanaik (2008), Drèze and Khosla (2008), and Adhikari and Bhattacharya (2010).
5. "There are 75 million homeless people in the country and a lot of nomadic people – all of them don't have an ID. We think UID will enhance their access to public services" (Chairperson Nandan Nilekani in *Indian Express*, 2009).
6. Intriguingly, the portability claim is repeated in at least four places in their paper on the PDS.
7. Since these claims have begun to be debunked, the UIDAI has responded by qualifying its statements. For instance in a recent *Teleika* interview, the problem of "no identity" was "referred to as a problem of "no mobile identity" (Vas 2010b).
8. The third category, i.e., inclusion errors (or misclassified cards), is known to be quite large. Since UID cannot fix that, I focus on duplicates and ghosts here.
9. Tamil Nadu has actually computerised operations so that it is possible to get real time stocks in each ration shop in the state. (Personal communication, MVS Mohi, managing director, Tamil Nadu Civil Supplies Corporation.)
10. In these scenarios, it is still possible for the dealer to "extort" grain after the coupon is deposited, or the card is swiped, or biometrics are authenticated. Yet it would mark an improvement in those areas where dealers can get away by saying that the grain has not reached him.
11. Inter-operability is another claimed benefit, but this benefits the government, not the claimant.
12. The Ministry of Rural Development has put out a Rs 2,162 crore tender for this purpose. See documents available online at http://nrega.nic.in/circular/eoi_concept.htm.
13. In this scenario, the UID becomes mandatory de facto – this is what "demand-driven" UID will translate into. The likelihood of labourers being explained

389
390

PERSPECTIVES

- that enrolment is voluntary seem somewhat ill-fitting especially in poorly governed parts of the country.
- 14 See Planning Commission (2010a and 2010b). Note again that even this model does not necessitate the use of a UID type database. It only needs biometrics or smart cards.
 - 15 See Mehrotra (2010). Several have made this suggestion, e.g., "I venture to say that Aadhaar will enable us to put in place a well-functioning social safety net for our citizens by unifying all subsidies into cash-based transfers" (Kelkar 2010).
 - 16 While no public statement has been made on transitioning to cash transfers in lieu of 'in kind' food transfers (such as PDS grains or mid-day meals), the government has announced the setting up of a committee, headed by Nilekani, to explore cash transfers instead of kerosene, LPG gas and fertiliser. According to newspaper reports, the basis for these cash transfers is a 'successful' pilot on smart cards being conducted in a few ration shops of Haryana (on the smart card pilots, see Narayan 2011a and 2011b). The current strategy seems to be to befuddle readers by using 'direct cash transfers', 'conditional cash transfers', 'smart cards', 'UID', 'biometrics' interchangeably to create the impression that these are the same or similar.
 - 17 In a sense, the UID project seems like a 21st century incarnation of the 20th century projects studied by James Scott (1998) in "Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed", where he highlights 'order' conditions common to all planning disaster: administrative ordering of nature and society by the state; a 'high-modernist ideology' that places confidence in the ability of science to improve every aspect of human life; a willingness to use authoritarian state power to effect large-scale interventions; and a prostrate civil society that cannot effectively resist such plans."
 - 18 "To give the United Kingdom as an example in relation to India is disingenuous. The stated goal of that scheme was surveillance and immigration control. They already have a number, which they started in 1953. Their ID card was a very different project. So let us not extrapolate randomly. The fact is that most countries have a number" (Nilekani in Vats 2010b).
 - 19 "The Identity Cards Bill outlines an identity system that has eight components: the National Identity Register, a National Identity Registration Number, the collection of a range of Biometric data such as fingerprints, the National Identity Card, provision for administrative convergence in the private and public sectors, establishment of legal obligations to disclose personal data, cross-notification requirements, and the creation of new crimes and penalties to enforce compliance with the legislation" (LSE 2005: 21).
 - 20 In response to the question "Isn't the main purpose security?", Nilekani said "You are right, the government in 2003 did modify the Citizenship Act to create the National Citizenship Register, which is now the National Population Register but that's primarily an initiative by the Registrar General of India. This government took an initiative to have a unique ID for developmental purposes. UIDAI came out of that initiative." See *Indian Express* (2009).
 - 21 One headline even touts it as the world's largest social inclusion initiative (Knowledge@Wharton 2010). However, as noted earlier, the unique number itself carries no welfare benefits.
 - 22 "Benefit fraud through false identity is relatively rare and we believe the cost of introducing an identity card in the benefits environment would far outweigh any savings that could be made" (LSE 2005: 10).
 - 23 "Under the proposed National Identification Authority of India Bill ('NIDAI Bill'), if someone finds that her 'identity information' is wrong, she is supposed to 'request the authority' to correct it, upon which the Authority 'may, if it is satisfied, make such alteration as may be required'. There is a legal obligation to alert the Authority but no right to correction!" (Drèze 2010).
 - 24 See *The Economist* (2010) and Pato and Millett (2010). See also Shukla (2010) who discusses the reliability of various biometrics error rates, costs, etc.
 - 25 The Chairperson of UIDAI is aware of the unprecedented scale of this project as is evident in this statement "This is a massively complex project as our biometric database will consist of 1.2 billion records which is 10 times larger than the current largest biometric record" (*Indian Express* 2009).
- ### REFERENCES
- Ahlikari, Anindita and Kartika Bhatia (2010) "NREGA Wage Payments: Can We Bank on the Banks?" *Economic & Political Weekly*, Vol 45, No 1, 2 January, pp 30-37.
- Ahasan, Hujumil, Philip O'Keefe, Cora Datta and Carlo del Ninno (2009) "Concept Note of a Smart Card Based Public Distribution System", presented by World Bank and CALZCAL Corporation.
- CalzCal (2008) "Concept Note of a Smart Card Based Public Distribution System", 22 August.
- Clara, Lewis (2010) "29 Lakh Fake Ration Cards Seized Last Year" *Times of India*, 9 February: <http://indiatimes.com/p/news-articles/times-of-india/the-india-20100209/29-lakh-fake-ration-cards-seized-20100209>.
- Debroy, Bibek (2013) "Where's the Privacy Bill?", *The Financial Express*, 28 September.
- Drèze, Jean (2010) "UID Unique Facility or Recipe for Trouble", *The Hindu*, 25 November.
- Drèze, Jean and Reetika Khera (2008) "From Accounts to Accountability", *The Hindu*, 6 December.
- (2010a) "The BPL Census and a Possible Alternative", *Economic & Political Weekly*, Vol 45, No 6, 27 February.
- (2010b) "Chhattisgarh Shows the Way", *The Hindu*, 13 November.
- Government of India (2010a) "UID and NREGA", UIDAI Planning Commission, Version 1, dated 24 June 2010. Available online at http://uidai.gov.in/UID_PDF/Working_Papers/UIDandNREGA.pdf.
- (2010 b) "Envisioning a Role for Aadhaar in the Public Distribution System", Working Paper, UIDAI, Planning Commission, Version 1, 24 June. Available online at http://uidai.gov.in/UID_PDF/Working_Papers/Circulated_Aadhaar_PDS_Note.pdf.
- (2010 c) "UID and the PDS System", UIDAI, Planning Commission, available online at http://uidai.gov.in/UID_PDF/Working_Papers/UIDandPDS.pdf.
- Gupta, Rishi (2010) "Justifying the UIDAI: A Case of Poorer Substance", *Economic & Political Weekly*, Vol 45, No 40, 2 October.
- Hirwar, Indira (2003) "Identification of BPL Households for Poverty Alleviation Programme", *Economic & Political Weekly*, Vol 38, No 45, 14 November.
- IANS (2010) "Delhi Has 65,000 Fake Ration Cards: Menus for the Poor, Court Told", *Times of India*, 21 July. Available online at <http://timesofindia.indiatimes.com/City/delhi/Delhi-has-65000-fake-ration-cards-meant-for-poor-court-told-/articleShow/6197368.cms>.
- Indian Express* (2009) "The Idea Is to Be Inclusive, The Upper and Middle Classes Have Many Forms of Identity, But the Poor Have None", The Idea Exchange, 20 November. <http://www.indianexpress.com/news/the-idea-is-to-be-inclusive-the-upper-and-middle-classes-have-many-forms-of-identity-but-the-poor-have-none/547510/>.
- Kelkar, Vijay (2010) "Solving the Identity Problem", *Times of India*, 27 November. Available online at <http://timesofindia.indiatimes.com/Home/opinion/edit-page/Solving-The-Identity-Problem/articleShow/5996221.cms>.
- Khera, Reetika (2006) "Access to the Targeted Public Distribution System: A Case Study in Rajasthan", *Economic & Political Weekly*, Vol 43, No 44, 1 November.
- (2010) "Not All That Unique", *Hindustan Times*, 30 September.
- Khera, Reetika and Muthiah Karuna (2010) "Slow But Steady Success", *The Hindu*, 25 April.
- Knowledge@Wharton (2010) "Nandan Nilekani on What It Takes to Build the World's Biggest Social Inclusion Programme", 4 November. Available online at <http://knowledge.wharton.upenn.edu/india/article.cfm?articleid=4541>.
- Krishna, Sudhir (2010) "Unique Identity Numbers: The Enabler of Policy Reform?", India in Transition, available online at <http://cas.usc.edu/indiaedu/it/krishnasudhir>.
- London School of Economics and Political Science (2005) *The Identity Project, An Assessment of the UK Identity Cards Bill and Its Implications* (London: London School of Economics and Political Science).
- Mahalingam, Anant (2009) "Sovereign States and Mobile Subjects: Politics of UIDAI", *Economic & Political Weekly*, Vol 44, No 46, 14 November, pp 35-40.
- Mehrotra, Santosh (2010) "Introducing Conditional Cash Transfers in India: A Proposal for Five CCTs", Planning Commission.
- Narayan, Swati (2011a) "Fingerprints Smart on the Scanner", forthcoming in *The Hindu*.
- (2011b) "Cards with 'Smarts'?", forthcoming in *The Hindu*.
- Nilekani, Nandan (2008) *Imagining India. Ideas for the New Century* (New Delhi: Penguin Books).
- Pato, Joseph M and Lynette I Millett, ed (2010) *Biometric Recognition. Opportunities and Challenges* (Washington DC: National Research Council).
- Planning Commission (2004) "A Study on the Effectiveness of Public Distribution System in Rural Tamil Nadu" by S Nakkiran, Planning Commission, Government of India. Available online at http://planningcommission.nic.in/reports/scereport/scr/std_pds'n.pdf.
- (2010a) "Towards a Workable Food Security Bill Discussion Paper by Planning Commission, Government of India.
- (2010b) "Comments on the Proposals of the NAC Working Group on Food Security", Planning Commission, Government of India.
- Radhakrishnan, R K (2010) "8 Lakh Bogus Ration Cards Cancelled", *The Hindu*, 29 August. Available online at <http://www.hindu.com/2010/08/12/stories/2010081255840400.htm>.
- Ramakumar, R (2010) "What the UID Conceals", *The Hindu*, 21 October.
- Ramanathan, Usha (2010a) "Implication of Registering, Tracking, Profiling", *The Hindu*, 5 April.
- (2010b) "Eyeing IDs", *Indian Express*, 1 May.
- (2010c) "A Unique Identity Bill", *Economic & Political Weekly*, Vol 45, No 30, 24 July, pp 10-11.
- Scott, James (1998) *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press).
- Sebastian, P T (2010) "The UID Task Has Just Begun", *Outlook Business*, 30 October.
- Sridharth and Vanaik Anish (2008) "Bank Payments: The End of Corruption?", *Economic & Political Weekly*, Vol 43, No 17, 26 April, pp 33-39.
- Srinama, R S (2010) "Identity and the UIDAI: A Response", *Economic & Political Weekly*, Vol 45, No 35, 28 August.
- Shukla, Ravi (2010) "Reimagining Citizenship: Debating India's Unique Identity Scheme", *Economic & Political Weekly*, Vol 45, No 2, 9 January, pp 31-36.
- Srinivasanathan, Madhura and Neeta Mishra (2001) "Errors of Targeting, Public Distribution of Food in a Maharashtra Village, 1995-2000", *Economic & Political Weekly*, 30 June.
- The Economist* (2010) "Biometrics, The Difference Engine Dubious Security", 1 October. Available online at <http://www.economist.com/blogs/bahibage/2010/10/biometrics>.
- Vats, Vaidhyan (2010a) "Why Nandan Wants to Tag You", *Telika*, Vol 7, Issue 44, 6 November. Available online at http://www.telika.com/story_main47.asp?filename=Neo61110Why_Nandan.asp.
- (2010b) "We Raised the Issue of Privacy Long before Anyone Else", *Telika*, Vol 7, Issue 44, 6 November. Available online at http://telika.com/story_main47.asp?filename=Neo61110We_raised.asp.



ATREE INVITES APPLICATIONS FOR INTERDISCIPLINARY PHD PROGRAMME IN CONSERVATION SCIENCE AND SUSTAINABILITY STUDIES

The Ashoka Trust for Research in Ecology and the Environment (ATREE), Bengaluru, invites applications for admission to its **Doctoral Research Programme**, recognised by Manipal University, for the academic year starting July 2011. Applications are invited from highly motivated students with a Master's degree in any branch of the social or natural sciences. Students will undergo intensive course work and will be expected to undertake independent research on any environmental topic under a multi-disciplinary Dissertation committee. Students are expected to join the programme full-time. Fellowship will be provided for at least 2 years of the programme.

Eligibility

1. Master's degree in any social or natural science or engineering discipline.
2. Must have qualified for one of the following entrance exams: UGC-CSIR (minimum NET), GATE, ICSSR, or equivalent qualifying exam OR have a M. Phil. degree OR have published at least one peer-reviewed paper as lead author or co-author OR have some demonstrated research ability OR based on evaluation of Statement of Research

Application

Candidates seeking admission for the PhD programme at ATREE should submit the following documents:

1. Completed application form (download from http://www.atree.org/phd_prog_2011)
2. Copy of degree certificate, provisional degree, or mark sheets from previous semesters of the completed Master's course
3. Written statement of research and career goals (up to 1000 words)
4. Confidential reference letters from two referees

The completed application form and supporting documents should be submitted by e-mail, post or fax to the address below by **April 25, 2011**. Please *superscribe* the envelope '**Application for PhD programme**'

Applicants who fulfill the eligibility requirements will be called for an interview at ATREE, Bengaluru after **May 10, 2011**. Detailed information on the PhD programme and research interests of the faculty can be obtained at http://www.atree.org/phd_program

About ATREE

ATREE was established in 1993 and is fast emerging as one of the South Asia's leading conservation and sustainable development research organisations, with a strong interdisciplinary emphasis. ATREE's research covers the broad themes of environment and development, biodiversity and conservation. Areas of specialisation include biodiversity conservation, environmental governance, ecosystem analysis and services, ecological agriculture, water management, urban environments and development and environmental change. Disciplines represented in the faculty (see <http://atree.org/faculty>) include ecology, taxonomy and eco-hydrology, landscape ecology and water resources as well as economics, development studies, sociology, history and political ecology. As the programme's broadens its focus, social sciences students with interest in environmental issues are particularly encouraged to apply.

ATREE fosters diversity and gender equity at the work place. Women and persons from underprivileged groups are especially encouraged to apply.

E-mail the completed application form to phd@atree.org, or post it to the address below:

The Coordinator

Academy for Conservation Science and Sustainability Studies

Ashoka Trust for Research in Ecology and the Environment (ATREE), Royal Enclave, Srirampura, Jakkur
Bengaluru, 560 064, India.

Email phd@atree.org, Phone: +91-80-23635555, Fax: +91-80-23530070

True Copy



De-duplication

The Complexity in the Unique ID context

1. Introduction

Citizens in India depend on the Government for various services at various stages of the human lifecycle. These services include issuance of birth certificate, voter identity card, ration card, driving license, passport, PAN card etc. In addition the government also implements different welfare schemes like Targeted Public Distribution System (TPDS), National Rural Employment Guarantee System (NREGS), health insurance, old age pensions etc for the economic and social upliftment of the people. A Unique Identity (UID) assigned for every citizen would obviate the need for a person to produce multiple documentary proofs of his identity for availing any government service, or private services like opening of a bank account. The Unique Identity (UID) would remain a permanent identifier right from birth to death of the citizen.

UID would enable government to ensure that benefits under various welfare programmes reach the intended beneficiaries, prevent cornering of benefits by a few people and minimize frauds. UIDs are also expected to be of help in law and order enforcement, effective implementation of the public distribution system, defining social welfare entitlements, financial inclusion and improving overall efficiency of the government administration

2. Enrollment

It is expected that the Government will enroll the citizens by capturing the Biographic and Biometric details and issue a Unique ID number. During the enrollment process, it has to be ensured that the same citizen does not get enrolled more than once. This can be done by comparing the biometrics of the citizen with all other citizens already enrolled and denying enrollment in case a match is found. Enrollment of citizens can be done in two ways.

- (i) The enrollment can be done online by adopting a centralized architecture, in which all the enrollment stations in the country are connected to the central server and the biometrics of the citizen being enrolled are matched / compared with the biometrics of all the citizens already enrolled. In case a match is found, the system will not allow enrollment to be done.
- (ii) The other way in which enrollment can be done is by adopting an offline enrollment method by synchronizing the data with the central server

342
393



periodically as and when internet connectivity is available or through regular backup of data by means of DVDs / Hard disks. The biometrics of the citizens captured through the offline method are then matched / compared with the biometrics of all other enrolled citizens at the central server to identify multiple enrollments of the same citizen.

What is important in both the cases is the **speed of matching** and the **accuracy of the matching** results. The speed of matching has to be very high as the number of citizens to be enrolled runs into millions. The accuracy is equally important as false matches will result in erroneous enrollments, delays and potential failure of the project itself. It is to be noted that, during the enrollment, the raw images of the biometrics are captured and algorithms are used for converting the images into templates which are used for comparison/ matching. The speed of matching and accuracy of matching depend on the biometric captured, the algorithm used and the matching engine deployed.

3. Biometrics

There are several Biometrics such as Fingerprints, Iris, Facial recognition, Hand Geometry, Signature, Voice patterns etc. which are being used by Governments all over the world for an extensive array of highly secure identification and personal verification solutions. Each of them has certain advantages and disadvantages which must be considered in developing biometric systems. Selecting the right biometric is critical to the success of any Identity Management project such as the Unique ID project. Key metrics that need to be evaluated for choosing a biometric include the stability of the biometric over the lifetime of a human being, Failure to Enroll (FTE) rate, False Accept Rate (FAR), and the False Reject Rate (FRR). It is important to understand the advantages and disadvantages of each biometric and the advantages of going in for Multimodal Biometric solutions

4. Multi-Modal Biometrics

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a single identification system. Biometric systems based solely on one-modal biometrics are often not able to meet the desired performance requirements for large user population applications, due to problems such as failure to enroll, noisy data, spoof attacks, environmental conditions and unacceptable error rates. Each of the biometrics has its' relative merits and applications where they can be used. A few examples are given below.

4.1 Face

The face can be the first form of identifying a person without the need for any external device; however, a facial recognition camera may not be able to distinguish between identical twins. Facial recognition works on the system identifying 9 geometric points on a human face and international studies have confirmed very high "False Acceptance Rates" (1 in 100).

4.2. Fingerprints

Fingerprints are ideal for verification (1:1 matching) though there are Automatic Fingerprint Identification Systems (AFIS) which do identification (1:N or N:N) also. However, even in the case of identification, the "False Acceptance Rates" are about 1:100,000.

- Fingerprint de-duplication is cost effective only for small population and the cost of de-duplication goes up significantly due to manual intervention required while doing de-duplication for huge population. This is due to large number of false matches thrown up during the fingerprint de-duplication process requiring Human intervention / Back office operations to work on the probable matches and thereby adding up to the costs;
- Fingerprints are susceptible to noisy or bad data, such as inability of a scanner to read dirty fingerprints clearly. People above 60 years and young children below 12 years may have difficulty enrolling in a fingerprinting system, due to their faded prints or underdeveloped fingerprint ridges. It is estimated that approximately 5 percent of any population has unreadable fingerprints, either due to scars or aging or illegible prints. In the Indian environment, experience has shown that the failure to enroll is as high as 15% due to the prevalence of a huge population dependent on manual labor.

However, the advantages of fingerprints are given below

- Fingerprint is cost effective at the time of verification. (Since at verification or the point of service, fingerprint devices of low cost can be used.
- Fingerprint can be used for forensic purposes.

4.3. Iris

- Iris recognition is the most accurate of the top three biometrics: fingerprints, facial recognition, and iris recognition. Iris recognition has a false accept rate of 1 in 1.2 million for one eye (1 in 1.44 trillion for two eyes) regardless of database size. As a result of the accuracy of Iris recognition, Iris returns a single result back. Fingerprint and face technologies generally return a



candidate list and then a manual process is required for resolving the candidate list. For this reason, Iris is the ideal biometric for applications which require real time identification. Processes such as fraud screen (to check for duplicates) enrolment for large populations can be easily handled by Iris recognition when they are very difficult for fingerprints.

- Iris recognition algorithms can search upto 20 million records in less than one second using a normal Quadcore – 2 Processor blade server. In a parallel process, using COTS hardware, Iris can perform at 1 billion matches per second. The ability to search a population database in real time and return a single match result is unique to Iris recognition technology. Due to manual candidate list resolution with face and fingerprint technologies, Iris is the only biometric which delivers operational results in real time which can be acted upon.
- Iris is an internal organ because of which there is no problem of environmental conditions affecting the Iris unlike finger prints which may not be prominent in people who do labor work or work in harsh environments (e.g factories, farms, etc).
- The Iris of a person is stable throughout a person's life (From the age of one year till death); the physical characteristics of the Iris do not change with age, diseases or environmental conditions. Hence one time enrollment is enough for a person during his lifetime.
- One of the most important advantages of using Iris as a Biometric is the lower effort, lesser infrastructure (servers, database licenses, datacenter infrastructure etc) required for de-duplication whereas finger print de-duplication requires more than 50 times infrastructure and more human effort. Another related cost that is normally overlooked is the infrastructure maintenance cost for running such as huge datacenter like, manpower, power consumption, annual maintenance costs for hardware and software etc.
- A comparative study of the performance of multiple biometrics done by the centre for Mathematics and Scientific Computing, National Physical Laboratory NPL of UK is given in the Table 1.

Table 1

| Biometric | FAR (False Acceptance Rate) | FRR (False Rejection Rate) | FER (Failure to Enroll rate) | Scalability | Stability |
|-----------------------|--------------------------------------|-------------------------------------|------------------------------------|---------------|----------------|
| Iris | 1:1.2 million | 0.1 – 0.2% | 0.5% | 1: all search | Very stable |
| Fingerprint | 1: 10(000) | 2.0 – 3.0% | 1.0 – 2.0% | 1: 1 match | Changes |
| Facial recognition | 1:100 | ~10% | 0.0% | 1:1 match | Changes |
| Hand Geometry | 1:10000 | 10 – 20% | 0.0% | 1:1 match | Changes |

For complete Report Please Refer - Biometric Product Testing Final Report (19 March 2001, Center for Mathematics and Scientific Computing, National Physical Laboratory, UK).

The most compelling reason to adopt Multi-Modal Biometric is to introduce certainty in the recognition process, real time identification, lower effort for de-duplication and reduce the possibility of inconvenience caused by malfunctioning of a single Biometric.

Advantages of using Multi-Modal Biometrics

- The enrollment cost for Multi-Modal Biometric enrollment will be about 5 – 10% marginally higher compared to single/dual biometric enrollment. However, the total cost of solution in case of multimodal enrollment is significantly reduced due to reduced cost during de-duplication which outweighs the marginal additional cost incurred during enrollment.
- Single biometric enrollment results in Failure to Enroll (FTE) if those biometric characteristics are absent in a citizen or if they are not qualified for enrollment (due to scars, aging or illegible/ worn out / cut / unrecognizable in case of fingerprints). In Indian conditions, where more than 60% of the population is involved in manual labour, experience has shown very high FTE rates for fingerprints.

5. De-duplication

De-duplication is the processing of the biometric data of citizens to remove instances of multiple enrollments by the same citizen. During de-duplication, matching the biometrics of a citizen is done against the biometrics of other citizens to ensure that the same person is not enrolled more than once. This will ensure that each person

396
397



will have a unique identity. De-duplication will be a necessary component in the "Unique ID" project. De-duplication is discussed in the context of the two different enrollment scenarios which are given below.

Case I: Enrollment using a centralized architecture

In the case of enrollment using a centralized architecture, the biometrics of the citizen have to be matched against the biometrics of all the previously enrolled citizens. The matching has to be done soon after the biometrics are captured to check whether the same citizen has been enrolled earlier. In case a match is found, the citizen will not be enrolled into the system. To accomplish this, the speed of matching has to be very high and without any false accepts. To illustrate the complexity, let us take a case where 200 million citizens have already been enrolled, and a new citizen is now waiting to be enrolled into the system at the enrollment station.

(1) When Fingerprints are used as the Biometric.

The number of matches to be performed and the time taken is shown in the table below.

| Scenario | No. of matches | Time taken (Assuming 10 blade servers with a total matching capacity of 5 m/100 per sec) |
|---|----------------|---|
| No. of matches if 1 finger (say left thumb) is matched against all left thumbs of previously enrolled citizens | 200 million | 40 secs |
| No. of matches if all 10 fingers are matched against the respective fingers of all the previously enrolled citizens | 2000 million | 400 secs (6.67 minutes) |
| No. of matches if all the 10 fingers are matched against all the fingers of all the previously enrolled citizens | 20000 million | 4000 secs (1.11 hours) |

(2) When Iris is used as the Biometric.

The number of matches to be performed and the time taken is shown in the table below.

397

398



| Scenario | No. of matches | Time taken (Assuming 100 blade servers with a total matching capacity of 200 million per sec) |
|---|----------------|--|
| No. of matches if 1 eye (say left eye) against all left eyes of previously enrolled citizens | 200 million | 1 sec |
| No. of matches if both eyes are matched against the respective eyes of all the previously enrolled citizens | 400 million | 2 secs |
| No. of matches if both eyes are matched against both eyes of all the previously enrolled citizens. | 800 million | 4 secs |

Thus it can be seen that the Iris based online enrollment is many times faster compared to the fingerprint based enrollment. Moreover, the fingerprint based De-duplication throws up false matches which have to be crosschecked with the photo or other parameters before deciding the accuracy of the match.

Case II: Enrollment using a De-centralized architecture

In the case of enrollment using a De-centralized architecture, the biometrics of citizens captured during a certain period have to be matched against the unique ID enrollment database of all the previously enrolled citizens. The matching has to be done by aggregating the data from each of the decentralized enrollment stations and matching against the de-duplicated biometrics of all the previously enrolled citizens. To illustrate the complexity, let us take the case where 200 million citizens have already been enrolled, and a data of 1 million citizens has been aggregated from the enrollment stations. The data of the 1 million citizens will have to be matched against the 200 million citizens to avoid multiple enrollments.

(1) When Fingerprints are used as the Biometric.

The number of matches to be performed and the time taken is shown in the table below.

398
399



| Scenario | No of matches | Time taken (Assuming 10 blade servers with a total matching capacity of 25 million per second) |
|---|----------------|---|
| No. of matches if 1 finger (say left thumb) against all left thumbs of previously enrolled citizens | 200 trillion | 463 days Or 1.27 years |
| No. of matches if all 10 fingers are matched against the respective fingers of all the previously enrolled citizens | 2000 trillion | 4630 days Or 12.67 years |
| No. of matches if all the 10 fingers are matched against all the fingers of all the previously enrolled citizens | 20000 trillion | 46296 days Or 126.84 years |

(2) When Iris is used as the Biometric

The number of matches to be performed and the time taken is shown in the table below.

| Scenario | No of matches | Time taken (Assuming 10 blade servers with a total matching capacity of 200 million per second) |
|--|---------------|--|
| No of matches if 1 eye (say left eye) against all left eyes of previously enrolled citizens | 200 trillion | 11.57 days |
| No of matches if both eyes are matched against the respective eyes of all the previously enrolled citizens | 400 trillion | 23.15 days |
| No of matches both eyes are matched against both eyes of all the previously enrolled citizens | 800 trillion | 46.30 days |

It can thus be seen that the decentralised enrollment will lead to large de-duplication times. By increasing the number of servers, it is possible to do the de-duplication within a day. To achieve the same timelines using fingerprints, it would

39c

L100



take 50 times the number of servers adopted for Iris based De-duplication. In addition to the increase in timelines and hardware, the number of false matches thrown up in Fingerprint based De-duplication would require large manpower to use other comparisons such as photos to eliminate the false matches.

6. Conclusion

Choosing the right biometrics plays a very important role for ensuring the success of the Unique ID project. While Iris as a biometric ensures high matching speeds and high degree of accuracy which are very essential for large Unique ID projects, fingerprint as a biometric will be economical for verification at the Point of Service. Thus the use of Multi-Modal biometrics will enable Governments to reap the advantages of both in the most optimal manner

UIDAI

Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

Biometrics Design Standards For UID Applications

Version 1.0
December 2009

Prepared by: UIDAI Committee on Biometrics

402

CONTENTS

| | | |
|------|--|----|
| 1 | EXECUTIVE SUMMARY..... | 4 |
| 2 | INTRODUCTION..... | 7 |
| 3 | OBJECTIVE..... | 8 |
| 4 | SCOPE..... | 9 |
| 5 | TARGET AUDIENCE..... | 10 |
| 6 | NORMATIVE REFERENCE..... | 11 |
| 7 | STANDARDS..... | 12 |
| 8 | TAILORING OF FACE IMAGE STANDARDS..... | 13 |
| 8.1 | SECTION 7 DIGITAL/PHOTOGRAPHIC REQUIREMENTS..... | 13 |
| 8.2 | SECTION 7 IMAGE COMPRESSION ALGORITHM..... | 13 |
| 8.3 | FACE RECORD FORMAT..... | 13 |
| 9 | TAILORING OF FINGER PRINT IMAGE STANDARD..... | 15 |
| 9.1 | SECTION 7: IMAGE ACQUISITION REQUIREMENTS..... | 15 |
| 9.2 | SECTION 8 FINGER IMAGE RECORD FORMAT..... | 15 |
| 10 | TAILORING OF MINUTIAE FORMAT STANDARD..... | 17 |
| 10.1 | SECTION 7.4.1.3 IMPRESSION TYPE..... | 17 |
| 10.2 | SECTION 7.5 EXTENDED DATA..... | 17 |
| 11 | TAILORING OF IRIS STANDARDS..... | 18 |
| 11.1 | SECTION 7.4.2.2 KIND..... | 18 |
| 11.2 | SECTION 7.4.2.4 IMAGE DATA..... | 18 |
| 12 | BEST PRACTICES..... | 19 |
| 12.1 | FACE..... | 19 |
| 12.2 | FINGERPRINT..... | 20 |
| 12.3 | IRIS..... | 21 |
| 12.4 | BIOMETRICS ACCURACY..... | 21 |
| 13 | MEMBERS..... | 23 |
| 13.1 | BIOMETRICS COMMITTEE..... | 23 |
| 13.2 | FACE SUB-COMMITTEE..... | 23 |
| 13.3 | FINGERPRINT SUB-COMMITTEE..... | 23 |
| 13.4 | IRIS SUB-COMMITTEE..... | 23 |
| | ANNEXURE I NOTIFICATION OF UIDAI CONSTITUTING THE COMMITTEE..... | 24 |
| | ANNEXURE II TECHNICAL DATA..... | 29 |
| | BIOMETRICS BASICS..... | 30 |
| | FACE..... | 30 |
| | FINGERPRINT..... | 30 |
| | IRIS..... | 30 |
| | FACE IMAGE BEST PRACTICES..... | 32 |
| | SUMMARY..... | 32 |
| | ENROLMENT..... | 32 |
| | AUTHENTICATION..... | 34 |
| | FINGERPRINT BEST PRACTICES..... | 35 |
| | SUMMARY..... | 35 |

| | |
|---|----|
| ENROLMENT..... | 36 |
| AUTHENTICATION..... | 37 |
| IRIS IMAGE BEST PRACTICES..... | 40 |
| SUMMARY..... | 40 |
| ENROLMENT..... | 41 |
| AUTHENTICATION..... | 43 |
| BIOMETRICS ACCURACY..... | 44 |
| STEP 1: ESTIMATING ACHIEVABLE ACCURACY..... | 44 |
| STEP 2: IMAGE QUALITY DIFFERENCE..... | 46 |
| STEP 3 COMPARISON & QUALITY ESTIMATES..... | 49 |
| CONCLUSIONS..... | 51 |
| FACE IDENTIFICATION..... | 52 |
| IRIS..... | 53 |
| FUSED ACCURACY..... | 53 |
| ISO DOCUMENTS..... | 55 |
| REFERENCES..... | 56 |

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standard.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable. These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

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

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is

data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion. Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.
2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.
3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.
4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.
5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.
6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

- 2405
406
7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.
 8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

506
L107

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards,, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

3 Objective

The UIDAI biometrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

2409
410

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint image Compression Specification 1997

ISO/IEC 15444 (all parts), information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6 3. Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022. (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at

http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

✓✓✓

U



1

412
413

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured

8.1.1 For Enrolment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

| Face Image Type Code | Scan resolution (dpi) | Color Space Code | Source Type Code | Inter-eye distance (pixels) | Facial Expression Code |
|----------------------|-----------------------|-------------------|------------------|-----------------------------|------------------------|
| Full Frontal (0x01) | 300 | 24 bit RGB (0x01) | 0x02 0x06 | 120 | 0x01 |

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

8.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

8.1.4 Pose

Roll, pitch and yaw angle should not be more than $\pm 5^\circ$ (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

8.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

413
414

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8.3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

414
415

3 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

3.1 Section 7. Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast over all response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

3.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

| Setting level | Scan resolution (ppcm) | Scan resolution (dpi) | Pixel depth (bits) | Dynamic range (gray levels) | Certifications |
|---------------|------------------------|-----------------------|--------------------|-----------------------------|----------------|
| 31 | 197 | 500 | 8 | 200 | EFTS/F |

3.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

| Setting level | Scan resolution (ppcm) | Scan resolution (dpi) | Pixel depth (bits) | Dynamic range (gray levels) | Certifications |
|-----------------|------------------------|-----------------------|--------------------|-----------------------------|----------------|
| 28 ¹ | 118 | 300 | 4 | 12 | UID |
| 30 | 197 | 500 | 8 | 80 | None |

3.2 Section 8 Finger Image record Format

3.2.1 Section 8.2.14 Image compression algorithm

3.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

3.2.1.2 Authentication

Code 4, compressed – JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

¹ Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

27/5
416

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 2 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification of this standard in bitmap is 7.5MB per subject.

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1 Impression Type

For enrolment image, only code² 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

² Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

417
418

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND_VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------|-------------------------------------|---------------|--|
| Enrolment | | | |
| | Image capture | R | Full frontal, 24 bit color |
| | Digital/Photographic requirements | R, S | Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. Inter-eye distance – minimum 120 pixels. |
| | Pose | S | Per ISO 19794-5 Section 7.2.2 |
| | Expression | R, S | Neutral expression. Specified as best practices. |
| | Illumination | S | Per ISO 19794-5 Section 7.2.7 |
| | Eye Glasses | S | Per ISO 19794-5 Section 7.2.11 |
| | Accessories | R | Permissible for medical and ethical reasons only. |
| | Multiple samples of face | M | Yes Recommended for automatic face recognition. |
| | Operational | S | Per ISO 19794-5 Section 7.2.4 - 7.2.10 |
| | Assistance | R | Yes. Specified as best practices. |
| | Segmentation and feature extraction | M | Recommended for automatic face recognition |
| | Quality check | R | Yes. Specified as best practice. |
| | Storage & compression | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted. |
| Authentication | | | |
| | Image capture | R | Same as enrollment |
| | Compression | S | JPEG 2000 color compression recommended. Compression ratio to be less than 10:1. |
| | Number of images | R | One full frontal image |

Figure 2 Face image

12.2 Fingerprint

| Key Decisions | | Decision Type ³ | Summary of Decisions |
|------------------------|-------------------------------|----------------------------|--|
| Enrolment | | | |
| Image capture | | | |
| | Plain or rolled | R | Plain, live scan |
| | Number of fingers | R | Ten |
| | Device characteristics | S | Setting level 31 or above, NIST/7 certified |
| | Quality check | R | Yes – specified as best practice |
| Operational | | | |
| | Assistance | R | Yes – Specified as best practice |
| | Corrective measure | R | Yes – Specified as best practice |
| Storage & transmission | | | |
| | Compression | S | Uncompressed images strongly recommended. For legacy reasons lossless JPEG 2000 or WSQ compression accepted. |
| | Storage format | S | Per ISO Section 8.3. No deviation necessary |
| | Minutiae format | S | Per ISO 19794-2. No deviation necessary. |
| | Multi-finger fusion algorithm | R | Recommended. Application dependent. |
| Authentication | | | |
| Image capture | | | |
| | Number of fingers | R | No minimum, no maximum. Application dependent. Recommended as best practice |
| | Any finger option | M | Yes Recommended as best practice |
| | Retry | R | Maximum 5. Recommended as best practice. |
| | Device characteristics | S | Setting level 28 or above |
| | Transmission format | S | Per ISO. No tailoring necessary |
| | Compression | S | JPEG 2000 compression recommended. Compression ratio to be less than 15:1 |
| | Minutiae format | S | Per ISO 19794-2. No tailoring necessary |

Figure 3 Fingerprint

³ R: Recommendation based on best practice/empirical data, S: Standard based, M: Management judgment.

12.3 Iris

| Decision | | Decision Type | Summary of Decision |
|----------------|------------------------|---------------|---|
| Enrolment | | | |
| | Image | R | Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter |
| | Device Characteristics | R | Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance > 300 mm for operator control, > 100mm enrollee control |
| | Operational | M | Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor. |
| | Segmentation | R | Non-linear segmentation algorithm |
| | Quality Assessment | R | Per IREX II recommendations ⁴ |
| | Compression & Storage | S | ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010). |
| Authentication | | R, S | Same as enrolment except One or two eyes JPEG 2000 KIND_CROPPED of Table A 1 |

Figure 4-165

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

⁴ IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

427
422

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes. Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.
2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.
3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.
4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

- Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.
- In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.
- The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

4-
423

13 Members

13.1 Biometrics Committee

| | Name, Affiliation |
|-----|---|
| 1. | Dr. B. K. Garola, DG NIC – Chairman |
| 2. | Dr. C. Chandramauli – Registrar General of India (RGI) – Member |
| 3. | Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member |
| 4. | Dr. A. M. Pedgaonkar, RBI – Member |
| 5. | Mr. Pravir Vohra, ICICI – Member |
| 6. | Prof. Deepak Phatak, IIT Bombay – Member |
| 7. | Prof. Phalguni Gupta, IIT Kanpur – Member |
| 8. | Mr. R. S. Sharma, DG UIDAI – Member/Convener |
| 9. | Mr. Rajesh Mashruwala, UIDAI – Member |
| 10. | Mr. Srikanth Nadhamuni, UIDAI – Member |

13.2 Face Sub-committee

| | |
|----|-----------------------|
| 1. | Dr. Richa Singh |
| 2. | Dr. Mayank Vatsa |
| 3. | Mr. Rajesh Mashruwala |

13.3 Fingerprint Sub-committee

| | |
|----|-----------------------|
| 1. | Prof. Phalguni Gupta |
| 2. | Dr. A. M. Pedgaonkar |
| 3. | Mr. Rajesh Mashruwala |
| 4. | Dr. Mayank Vatsa |

13.4 Iris Sub-committee

| | |
|----|-----------------------|
| 1. | Prof. Phalguni Gupta |
| 2. | Dr. Mayank Vatsa |
| 3. | Mr. Rajesh Mashruwala |

64A
424

Annexure I

Notification of UIDAI constituting the Committee

As UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in (UID) applications, mostly/exclude/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation in view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/exclude/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of biometrics. Personal Identification and Location Codification Standards. These committees have worked out low standards in the respective categories to be uniformly applied for various e-governance standards.

UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in (UID) applications, mostly/exclude/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation in view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/exclude/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication.

OFFICE MEMORANDUM

Dated: September 29, 2009

To: Mr. C. V. Venkatesh
New Delhi - 110 001

Unique Identification Authority of India
Planning Commission
Government of India
No. 45/D-UIDAI/2009

425
444

1. Charter of the Biometric Standards Committee

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the UID system.
- To review the existing standards of Biometric and, if required, modify/extend/replace them so as to serve the specific requirements of UIDAI relating to Identification and Authentication

2. Composition of the Biometric Standards Committee

Following will be the composition of the Biometric Standards Committee.

1. Dr. B.K. Chandra - Director General, National Informatics Centre - Chairman
2. Dr. C. Chandrasekhar - Registrar General of India - Member
3. Dr. T.S. Gangwar, Jt Secretary, Min of Rural Development - Member
4. Dr. A.M. Padgugolite, Reserve Bank of India - Member
5. Mr. Pravin Vora, CICA - Member
6. Dr. Deepak Phatak, IIT Bombay - Member
7. Dr. Pradipni Gupta, IIT Kanpur - Member
8. Two representatives from Technology Team of UIDAI - Members
9. Director General, UIDAI or his Nominee - Member/Convener

Unique Identification Authority of India (UIDAI) will service this Committee.

The Committee will be able to invite representatives from user organisations and other Technology Experts as Special Invited to solicit their views and advice on various aspects on the issue

3. Technical Committee and Working Groups

The committee can also set up sub-committees that focus on various aspects of Biometric standards such as fingerprints, Iris and facial image and working groups for conducting/developing reference implementations/proof of-concept (POC) studies, specific research, field testing etc. on an as-needed basis. The Committee may meet from time to time and draft the standard document based on the feedback of sub-committees and working groups and submit recommendations. The Committee may also set its own review process before recommending the final standards.

4/26
4.23

Working Groups can be created to assist the above committee, by conducting proof-of-concept (POC) studies, specific research, field testing (tc).

4. Review process

It is important that the standards remain unbiased, pragmatic, vendor neutral, interoperable, and cost effective in biometrics where technology continues to progress rapidly, three parties - vendors, academia and enterprise users - have great deal of knowledge of the technology. The Committee's review process will leverage their knowledge without compromising on its charter

The technical committee will publish a draft version of the document and solicit structured feedback from the members of the committee, technology vendors, academia and enterprise users. Such review process will also provide sufficient advance notice to the vendors to begin upgrade to their solution, thus reducing lead time between the final standards adoption and conforming solutions.

The feedback from the various groups will be reviewed by the technical committee and suitable changes made in order to incorporate useful inputs. The final draft will be sent over for a final review and then the ratified version of the standards will be released.

5. Deliverables of the committee

- Obtain consensus from Government stakeholders to adopt and use a common set of standards for interoperability, containment of biometrics system cost and wide spread propagation of Biometrics in governmental and private sectors.
- Review the existing standards of Biometric and if required, modify/extend/enhance them so as to serve the specific requirements of UDAI relating to de-duplication and Authentication.
- Ratify biometrics standards from applicable base Indian and International standards, which meet needs of the UDAI.
- Recommendation to UDAI users to assure interoperability of biometrics data.
- Develop certification criteria for conformity, interoperability and performance
- Maintain & Publish registry of recommended biometrics standard, interoperability recommendations and certification criteria.

427
428

6. Time-Frame

Keeping in view the commitment of UIDAI to start issuing UID's within twelve to eighteen months, it is necessary that the Committee presents its report on standards as early as possible. Hence the Committee will present its Final Report to the undersigned on Biometric Standards to be adopted by UIDAI within 90 days of its constitution.

7. Miscellaneous

The non-official members of the Committee and Special invitees will be reimbursed the cost of their travel and other incidental expenses as per Rules as and when they travel to attend the Committee meetings.

Dr. R. S. Sharma

(R. S. Sharma)
Director General & Mission Director

Copy forwarded to the Chairman and Members of the Committee for information and necessary action.

Copy to Cabinet Secretary / Principal Secretary to the PM/AT Secretaries to Govt. of India/All Chief Secretaries of the States/UTs for information

~~428~~

429

Annexure II Technical Data

49
430

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible [1].

Demographic data is used along with the biometric information to improve the de-duplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in de-duplication. It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general, it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images. Fingerprints also lend themselves very well to forensic investigation.

There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or more fingers [5].

Fingerprint technology constitutes approximately half of the total biometrics market⁵.

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore the iris would be a good biometric for pure de-

⁵ IDC & Acuity Market Research Reports.

duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired. Iris has no association with law enforcement and has not received negative press and may therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of the iris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

| Biometric identifier | Reference | FRR | FAR |
|----------------------|------------|-------|-------|
| Fingerprint | NIST FpVTE | 0.1% | 1% |
| Face | NIST FRVT | 10% | 1% |
| Voice | NIST 2004 | 5-10% | 2-5% |
| Iris | ITIRT | 0.99% | 0.94% |

Figure 5 FAR and FRR error rates

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------|-------------------------------------|---------------|---|
| Enrolment | | | |
| | Image capture | R | Full frontal, 24 bit color Inter-eye distance - minimum 120 pixels. |
| | Digital/Photographic requirements | R, S | Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. |
| | Pose | S | Per ISO 19794-5 Section 7.2.2 |
| | Expression | R, S | Neutral expression Specified as best practices. |
| | Illumination | S | Per ISO 19794-5 Section 7.2.7 |
| | Eye Glasses | S | Per ISO 19794-5 Section 7.2.11 |
| | Accessories | R | Permissible for medical and ethical reasons only. |
| | Multiple samples of face | M | Yes. Recommended for automatic face recognition. |
| | Operational | S | Per ISO 19794-5 Section 7.2.4 - 7.2.10 |
| | Assistance | R | Yes. Specified as best practices. |
| | Segmentation and feature extraction | M | Recommended for automatic face recognition |
| | Quality check | R | Yes. Specified as best practice. |
| | Storage & compression | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted. |
| Authentication | | | |
| | Image capture | R | Same as enrolment |
| | Compression | S | JPEG 2000 color compression recommended. Compression ratio to be less than 10:1. |
| | Number of Images | R | One full frontal image |

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with enrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

Pose

Face image should be full frontal with 0° of yaw, pitch and roll angles. However, in operational conditions, variation of $\pm 5^\circ$ is permissible.

Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons.

Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints, automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image with yaw, pitch and roll angle as 0° . The other two images should be left and right semi profile with yaw as $\pm 20^\circ$ to $\pm 30^\circ$, and the roll and pitch should be 0° .

Operational

Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction

Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check

Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression

According to Figures 12 and 13 of IIO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image it is strongly recommended that uncompressed images should be stored in the database.

Authentication

The authentication process consists of steps similar to enrolment.

Image Capture

Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression

For verification, images with JPEG 2000 compression ratio of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

434,
435

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?
 2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?
 3. Management judgment (M): Management decision based on project context.
- The remaining section has a brief explanation of each decision.

| Key Decisions | | Decision Type | Summary of Decisions |
|-----------------------------------|-------------------------------|---------------|--|
| Enrolment | | | |
| | Image capture | | |
| | Plain or rolled | R | Plain, live scan |
| | Number of fingers | R | Ten |
| | Device characteristics | S | Setting level 31 or above, EFTS/F certified |
| | Quality check | R | Yes - specified as best practice. Avoid NFIQ quality 4 and 5 level fingerprints. |
| Operational | | | |
| | Assistance | R | Yes - Specified as best practice |
| | Corrective measure | R | Yes - Specified as best practice |
| Storage & transmission | | | |
| | Compression | S | Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted. |
| | Storage format | S | Per ISO Section 8.3. No deviation necessary |
| | Minutiae format | S | Per ISO 19794-2. No deviation necessary |
| | Multi-finger fusion algorithm | R | Recommended. Application dependent. |
| Authentication | | | |
| | Image capture | | |
| | Number of fingers | R | No minimum, no maximum. Application dependent. Recommended as best practice |
| | Any finger option | M | Yes. Recommended as best practice |
| | Retry | R | Maximum 5. Recommended as best practice. |
| | Device characteristics | S | Setting level 28 or above |
| | Transmission format | S | Per ISO. No tailoring necessary |
| | Compression | S | JPEG 2000 compression recommended. Compression ratio to be less than 15:1 |
| | Minutiae format | S | Per ISO 19794-2. No tailoring necessary |

Figure 7 Fingerprint

435
436

Enrolment

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computationally intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural workers, the Committee recommends capturing prints of all ten fingers, the maximum possible

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images⁶. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

⁶ It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. **Operator Assistance:** Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.
2. **Corrective measures & retries:** If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence. Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for de-duplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

Image capture

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

438
439

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use "standard" minutiae data.

439
440

Iris Image Best Practices

Summary

Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture.

Figure 8 summarizes key decisions for UIDAI iris design.

| Decision | | Decision Type | Summary of Decision |
|----------------|------------------------|---------------|---|
| Enrollment | | | |
| | Image | R | Two eyes > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter |
| | Device Characteristics | R | Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance > 300 mm for operator control, > 100mm enrollee control |
| | Operational | M, R | Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor |
| | Quality Assessment | R | Per IREX II recommendations ⁷ |
| | Compression & Storage | S | ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010). |
| Authentication | | R, S | Same as enrollment except One and/or two eyes JPEG 2000 KIND_CROPPED of Table A.1 |

Figure 8 Iris

The remaining section has a brief explanation of each decision.

⁷ IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

Enrollment

Two Eyes

Capture of two eyes simultaneously provides several advantages⁸. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality.

In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and at least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the "capture volume") within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range.

⁸ Material derived from [32]

6447
442

The iris image capture sensor shall use progressive scanning.

In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 10 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris. The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ratio of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.

One method widely used for ensuring good iris images is recommended here. An Iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images and use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

442

443

Authentication

For 1:1 verification, any one eye will suffice, though application may require higher-level assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to `KIND_CROPPED_AND_MASKED` or `KIND_CROPPED` using JPEG 2000. Resulting image size will be between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design of the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade-off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

- Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.
- Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.
2. Estimate difference in image quality between Western and Indian conditions.
3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples. It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

| Shape Filter | Thresholds 1300, 1880 | | Thresholds 1400, 2025 | | Matches per Second |
|--------------|-----------------------|-------|-----------------------|-------|--------------------|
| | FAR | TAR | FAR | TAR | |
| Off | 0.30% | 96.3% | 0.07% | 95.6% | 734K |
| On | 0.32% | 96.1% | 0.07% | 95.5% | 1035K |

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

- False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.
- False Rejection Rate does not vary over gallery size as shown in Figure 12.
- Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of

approximately $0.07 \times 200 = 14\%$. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

- Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

| Number of Fingers | FRR % | FAR % |
|-------------------|-------|-------|
| 2 | 10.3 | 29.2 |
| 10 | 10.9 | 0.0 |

Figure 10 Accuracy to multiple fingers

- Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expected to be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of FAR 1.4% at FRR rate of 2%. In other words, NIST data indicates de-duplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

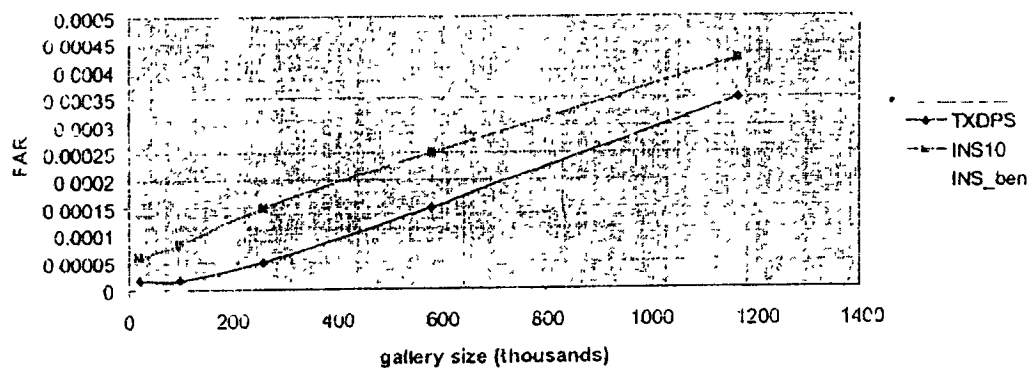


Figure 11 FAR as function of gallery size

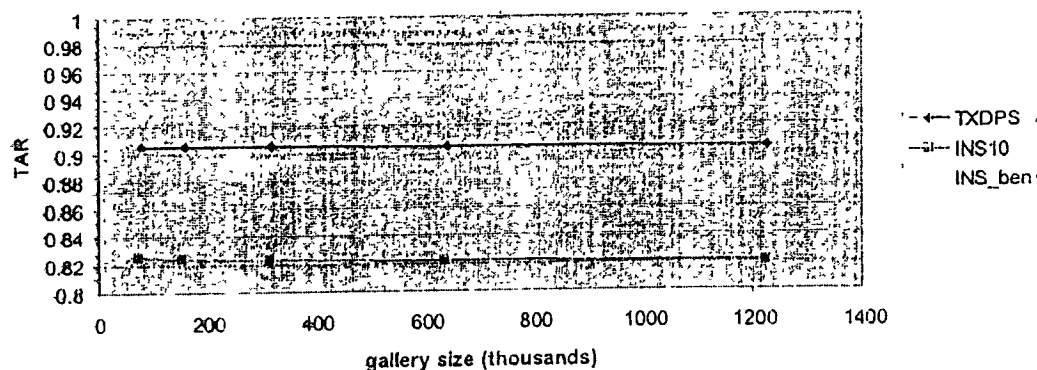


Figure 12 TAR as function of gallery size

2/13
446

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or 20% false accept rate).

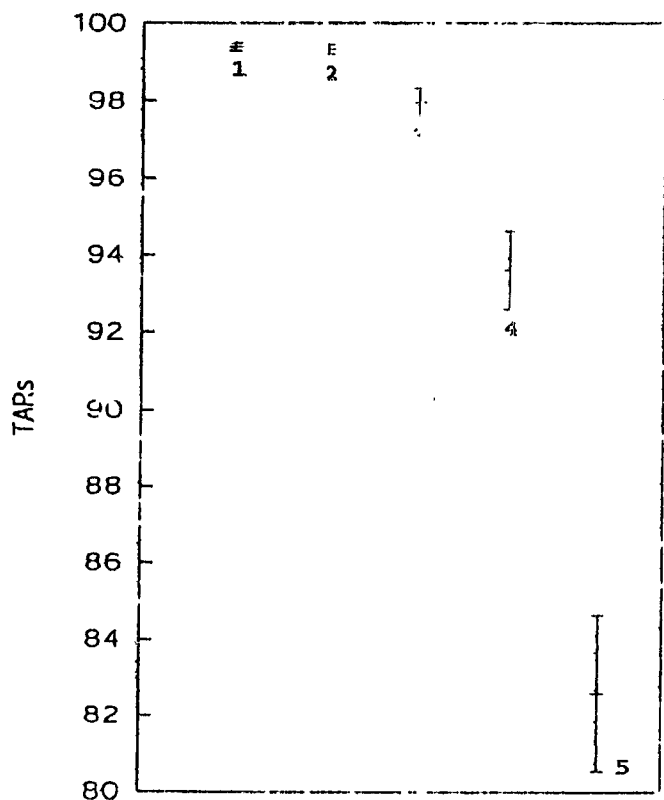


Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

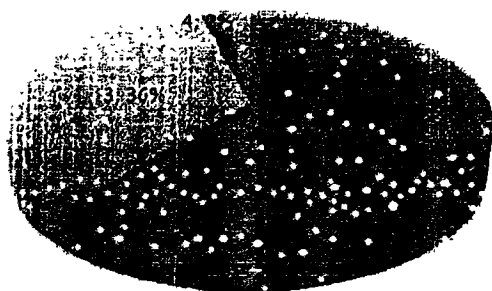


Figure 15 US-VISIT image quality distribution for right index finger

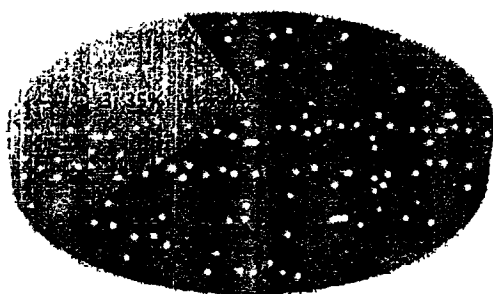


Figure 16 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained from diverse, disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases, fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). This database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.
2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.
3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software (NFIQ), images were classified in to bins according to the image quality score. The bin

distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5 numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

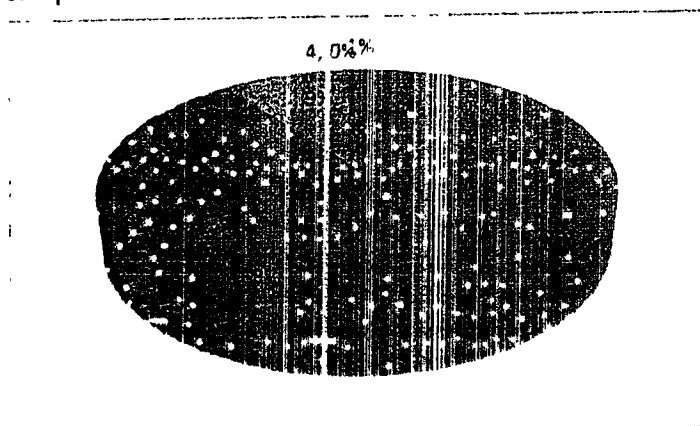


Figure 16 Image quality score distribution for DB1 Urban sample

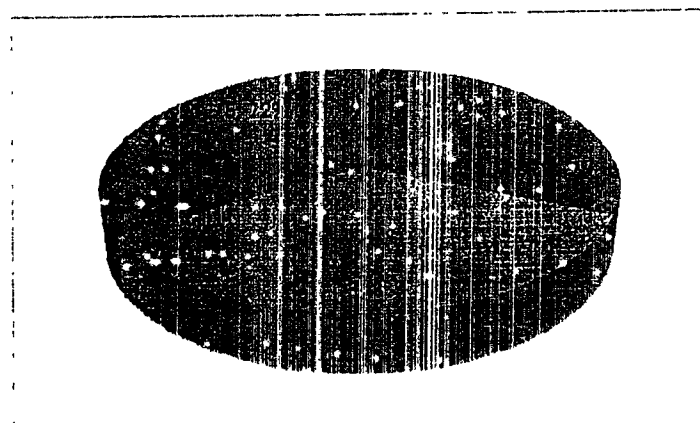


Figure 17 Image quality score distribution for DB1 Rural sample

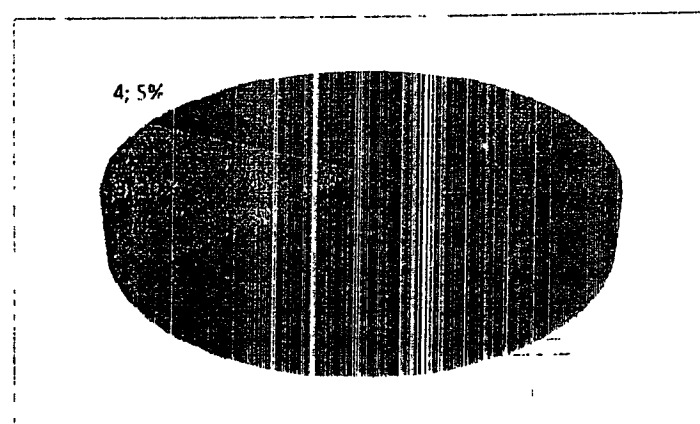


Figure 18 Image quality score distribution for DB2

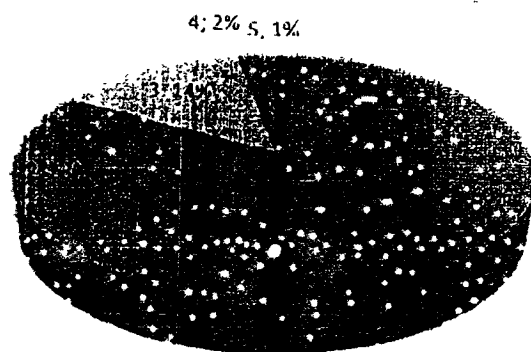


Figure 19 Image quality distribution for DB3

step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, using existing Western results[24], it is possible to closely predict the expected fingerprint recognition performance.

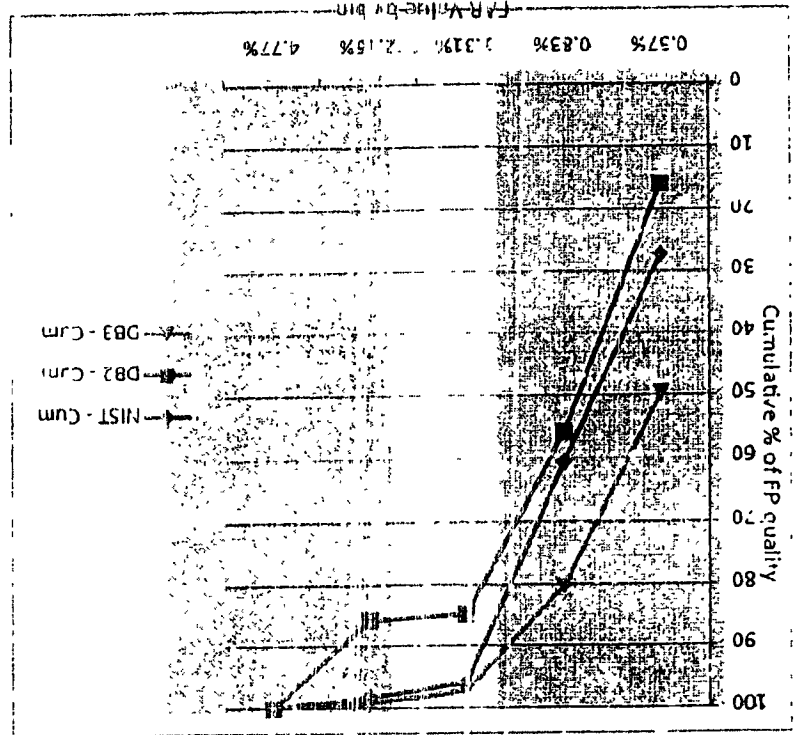
Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Western curve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

| Source | Bin 1 | Bin 2 | Bin 3 | Bin 4 | Bin 5 |
|------------|-------|-------|-------|-------|--------|
| NIST | 27.28 | 33.32 | 35.37 | 2.23 | 1.8 |
| NIST - Cum | 27.28 | 60.9 | 95.97 | 98.2 | 100 |
| DB2 | 15.87 | 40.03 | 28.88 | 0.99 | 14.11 |
| DB2 - Cum | 15.87 | 55.95 | 84.83 | 85.82 | 100.00 |
| DB3 | 49.73 | 30.51 | 16.97 | 2 | 0.79 |
| DB3 - Cum | 49.73 | 80.24 | 97.21 | 99.21 | 100.00 |

Figure 21 Right index finger numerical data

Figure 20 Right index finger comparison



Handwritten signature/initials

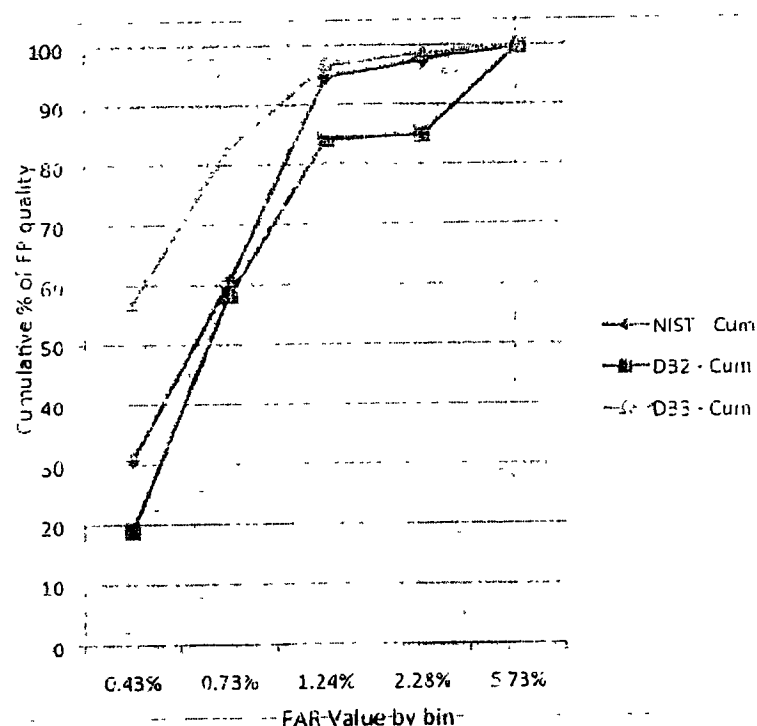


Figure 2.5 Left index finger comparison

| Source | Bin 1 0.43% | Bin 2 0.73% | Bin 3 1.24% | Bin 4 2.28% | Bin 5 5.73% |
|------------|----------------|----------------|----------------|----------------|----------------|
| NIST | 30.83 | 29.78 | 34.08 | 2.88 | 2.43 |
| NIST - Cum | 30.83 | 60.61 | 94.69 | 97.57 | 100 |
| DB2 | 18.99 | 39.36 | 25.87 | 0.90 | 14.88 |
| DB2 - Cum | 18.99 | 58.35 | 84.22 | 85.12 | 100.00 |
| DB3 | 57.25 | 25.77 | 13.8 | 1.87 | 1.31 |
| DB3 - Cum | 57.25 | 83.02 | 96.82 | 98.69 | 100.00 |

Figure 2.5 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performance of fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

- The UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. There is good evidence to suggest that Indian rural data may be as good as developed country settings when proper operational procedures are followed and good quality devices are used.
- It is possible to closely predict the expected fingerprint recognition performance. In the experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for $Q = 1, 2$, and 3 , 99% TAR with about 1% FAR).

- 45
- It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:

1. Using wet towels to remove dirt and moisten dry fingers
2. Using minimum quality threshold to ensure that extra efforts are made to capture good prints from hard to obtain fingers and
3. Keeping scanning devices in operational order

These resulted in exceptionally good bin 1 and 2 distribution.

- It is also observed that the slap fingerprint segmentation tools require some prior training for Indian databases. After some training, segmentation results improve by 2-3%. This also suggests that in deploying a biometrics (fingerprint) system, a carefully designed a priori training set and procedure will help in improving performance.
- Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.
- When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub continental region compared to Western and European countries. *Lawsonia inermis* (commonly known as henna or mehandi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and when applied, fingerprint sensors may not properly capture fingerprint features.
- On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the latter, gallery size is small, typically 1% of database. The hierarchical method improves FRF (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

452
453

Fig 24

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample

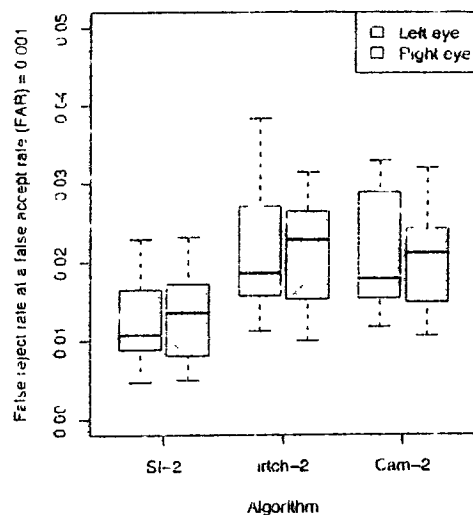


Figure 24: iris FAR & FR rate

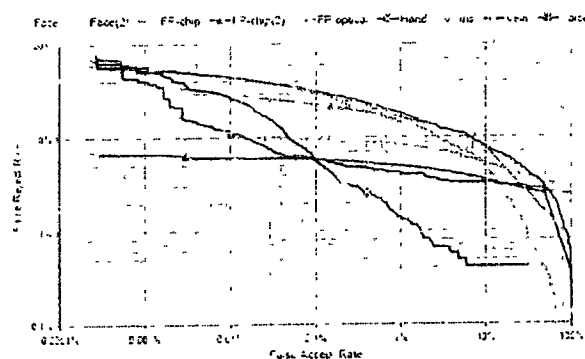


Figure 25: FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety of fields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupta and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities,

453
454

combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

4.54
4.55

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006
2. Anil Jain, Patrick Flynn, Arun Ross, Handbook of Biometrics 2008
3. ANSI/NIST-ITL 1-2007, American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1
4. ANSI/NIST-ITL 2-2008, American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2 XML Version
5. Bolle, Connell et al. Guide to Biometrics 2004
6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft Version 0.4, National Information Center
7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing (ICSIP 2006), Karnataka, India, 2006
8. IAFIS-IC-0100 (v7) Electronic Fingerprint Transmission Standard (EFTS) 1999
9. International Biometrics Group, "Independent Testing of Iris Recognition Technology, Final Report, May 2005", NBCHC030114/0001. Study commissioned by the US Department of Homeland Security
10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629
11. ISO/IEC 19784-1:2006, Biometric Application Programming interface – Part1: BioAPI specification.
12. ISO/IEC 19794-1:2006, Biometric data interchange formats – Part 1: Framework
13. ISO/IEC 19794-5:2005, Biometric data interchange formats – Part 5: Face image data
14. ISO/IEC 19794-6:2005, Biometric data interchange formats – Part 6: Iris image data
15. J. Cambier, "Iridiar Large Database Performance", Iridian Technical Report 03-002
16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006
17. J. Daugman, "Iris recognition border crossing system in the UAE", International Airport Review (2) 2004.
18. J. Daugman, Technical Report 635, University of Cambridge, 2005
19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005
20. Jonathon Phillips, "ICI 2006 Large-Scale Results", NIST 7208, NIST, 2007
21. NISTIR 7110, Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints. C. L. Wilson, M. D. Garriss, & C. I. Watson, May 2004
22. NISTIR 7112, Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATE). Stephen S. Wood & Charles L. Wilson, April 2004
23. NISTIR 7123, Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, Charles Wilson etc al.
24. NISTIR 7151, August 2004 Fingerprint Image Quality
25. NISTIR 7201, Effect of Image Size and Compression on One-to-One Fingerprint Matching. C. I. Watson & C. L. Wilson. February 2005

456
457

26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C. Wilson, M. Indovina & B. Cochran. July 2005
27. NISTIR 7296. MINEX. Performance and Interoperability of the INCI TS 3 7 8 Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006
28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007
29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4, April 2007.
30. Registry of USG Recommended Biometric Standards, Version 2.0, NIST C
31. Report of the working group on standards for raw images of fingerprints, Reserve Bank of India
32. Shahram Orandi, Mobile ID Device Best Practice Recommendations, NIST Special Publication 500-280, August 2009
33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex TW11 0LW
34. UK Passport Service, Biometrics Enrolment Trial, May 2005

True Copy
F
Adv

SEARCH

GO

Exh-S
16/10/12
4

[Home](#) [News](#) [Opinion](#) [Sport](#) [Business](#) [Arts](#) [Life & Style](#) [S & T](#) [Education](#) [Health](#) [Jobs](#) [Classifieds](#) [Today's Paper](#)
[Topics](#)

[International](#) [National](#) [States](#) [The India Cables](#) [The Pakistan Cables](#)

Cities: [Coimbatore](#)

[News](#) » [Cities](#) » [Coimbatore](#)

Published: October 31, 2011 10:08 IST | Updated: October 31, 2011 10:13 IST COIMBATORE, October 31, 2011

Aadhaar card must for LPG refills

V. S. Palaniappan

[Share](#) · [Comment](#) (19) · [print](#) · [T+](#) [T+](#)

Consumers to be given time to comply with Ministry order

The Ministry of Petroleum and Natural Gas has brought in an amendment to its Liquefied Petroleum Gas (Regulation of Supply and Distribution) Order 2000 making the Unique Identification Number (UID) under the Aadhaar project must for availing LPG refills.

The move is aimed at preventing multiple connections and availing cylinders in third party name and to clean up the LPG consumer base, as the government was spending heavily on subsidising the domestic LPG cylinders.

With people not showing keen interest in availing the UID or Aadhaar cards, the move of the Petroleum and Natural Gas Ministry is expected to increase the enrolment for Aadhaar.

The Ministry in its circular dated October 13, 2011 has announced the amendment to the LPG Regulation of Supply and Distribution order 2011. The Ministry's decision to make Petroleum Corporations sensitise distributors on Aadhaar card for availing refills has been published in the Gazette of India vide notification dated September 26.

The order has come into effect from the date of publication of the gazette notification.

The decision to make Aadhaar UID mandatory has been taken by exercising powers conferred under Section 3 of the Essential Commodities Act of 1955 (10 of 1955).

The amended order reads as follows: No distributor of a Government Oil Company shall supply LPG cylinder to any household unless the head of such a household furnishes Aadhaar number of each member of his or her household to the distributor within three months from the date of notification of such area.

Notification of such area means an area notified for enrolment for availing Aadhaar number. Many major towns in Western Tamil Nadu came under Aadhaar enrolment notification in June and July of 2011.

Officials of the Oil Corporations in Western Tamil Nadu when contacted said that distributors had been asked to sensitise consumers on the need for availing the Aadhar number at the earliest for availing uninterrupted supply of LPG refill.

Consumers will be given reasonable time to comply with the directive.

Keywords: LPG supply, Aadhaar card

Share

Ads by Google

LIC Pension 1.45 करोड़

छोटा निवेश जो आपको करोड़पति बनाये = Pension

PolicyBazaar.com/PureInvestment

Related

NEWS

2-cr. Aadhaar numbers issued in October 'Set up computerised back-office for PDS by April' Manpower shortage hits Aadhaar enrolment

TOPICS

India Tamil Nadu

Comments:

Sir, Recently only Aadhaar card is being spoken and hardly a very few are aware of this card. The Government has not taken swift action to educate the importance of this in urban areas, how could they effective action against LPG refill supply. It is going to create hardship to the public at large. Like Ration card Government should go about canvassing house to house before implementing action.

from: Ramachandran.J

Posted on: Oct 31, 2011 at 19:07 IST

The process of taking the sick and very old people to Aadhaar centres is going to be an extremely difficult task. Hence Aadhaar numbers should not be insisted upon for the gas connections owned by them.

from: Devarajan

Posted on: Nov 1, 2011 at 02:15 IST

The report would have been more complete if only the details of the areas in Tamil Nadu, so far notified, had been listed out. Can you please carry this information in your publication?

from: V Guruprasad

Posted on: Nov 1, 2011 at 06:42 IST

I had fixed up appointments for my Aadhaar Card with M/s Kary Consultants, T Nagar Chennai for the 15th Sept. When I went to their office at the scheduled time with my wife, they informed me that there were some technical issues and would call us back after 3-4 days. It is one and a half months since and we are yet to be called. This is the state of affairs of the project. The Government is doing its maximum to inconvenience the common man. We suffer in silence.

from: P M Vijayaraghavan

Posted on: Nov 1, 2011 at 06:44 IST

Here we go again! What is wrong with the oil marketing companies - why do they keep inventing new ways to harass the consumers? The trouble we were all put to a few years ago when they insisted on ration cards to identify 'genuine' user is still fresh in my mind because it involved running from pillar to post to get a ration card just to make a cup of coffee! and now this when it is not mandatory. Can they first cut down the number of free cylinders and connections given to all MLAs and MPs? That should make plenty available to all of us - common, tax-paying citizens without strings and 'connections'!

from: Vichitra PK

Posted on: Nov 1, 2011 at 12:51 IST

As an NRI who comes home on vacation once a year, where would I get my gas cylinder from? To have to get an Aadhaar card first and then book for a cylinder refill would delay my first cup of coffee by a few days if not weeks. Is there no other way to identify the abusers of the system? How would this affect the new pricing policy touted where customers need to pay a higher price for LPG cylinders beyond the subsidized quota? Do we still need Aadhaar cards for that as well? The more control you bring into the system, the more prone we become to corruption in a country like ours.

from: Mathew PG

Posted on: Nov 2, 2011 at 09:11 IST

govt should give more information and arrange for awareness programme before implementing for any availment of the commodities.

from: senthilkumar

Posted on: Nov 2, 2011 at 11:23 IST

It is not known whether Aadhaar number is being issued to Chennai city and if so who is to be contacted. Such details are not known to public through media or not even posted in Aadhaar web site. It appears if this trend continues, it may take several years to issue Aadhaar number to all Indians.

461
460

from: R.Ganesan.

Posted on: Nov 2, 2011 at 18:34 IST

Govt. very slow and not much interested in making public for Aadhar. How many advts are released for Aadhar ? First move should be made by the GOVT for publishing this and it should be made mandate. Very good initiative taken by govt. but very less awareness in public because no one knows where we get this and how to get it and what are the advantage or necessity of getting this cards.

from: Venkatesh

Posted on: Nov 3, 2011 at 16:11 IST

Whats the difference between Aadhar & UID? (This is the state of affairs in the common man's mindset now). Advertisements on a major scale is needed before implementing any new laws. Common man should not be affected. Why not government embrace the power of IT? So, people can still carry on their normal lives and also complete the formalities to get this card be it UID or Aadhar or Ration or PAN or Aavin card or whatever.

from: Ram

Posted on: Nov 4, 2011 at 13:10 IST

Aadhar card issuing authorities should be join a position to utilise the list of residents with election commission authorities and the aadhar prepared in accordance with that in advance and request the residents to come and collect it. Under any circumstances the culture of come-tomorrow should be avoided by concerned authorities, and avoid putting elders in difficulties.

from: C.K.Pandarinathan

Posted on: Nov 7, 2011 at 11:40 IST

really the government is harassing the old people, sick people and those who are tenants having no registered rent agreement but having unregistered rent agreement. .

from: M Subramanian

Posted on: Nov 9, 2011 at 11:59 IST

Aadhar card should have language of choice of the people and not Hindi alone. This should not be used as another political or discriminatory tool by the central government.

from: Selvan

Posted on: Nov 10, 2011 at 16:35 IST

Making UID cards mandatory is not fair because the ration card which is a valid document has been in force to get an authorised domestic connection. Further, why make the life of the common man and the regular honest tax assesse all the more complicate ?

from: hema ravi

Posted on: Nov 15, 2011 at 15:21 IST

I don't see any reason why NRI is making fuss about this arrangement. In our country each and every rule brought by the beauracrats is to make money. If you pay extra 50 Rs, even the CEO of oil company will deliver

1/16/12

The Hindu : Cities / Coimbatore : Aadhaar card must for LPG refills

464

the cylinder to your door step with utmost respect, in a highly corrupted India. All rules and laws is only to torture the havenot's not for rich people.

from: R.Manivarmane

Posted on: Nov 15, 2011 at 16:15 IST

Where and how to apply Aadhar card for Pallavaram area (Kancheepuram District)

from: R. Nisha

Posted on: Nov 16, 2011 at 12:37 IST

Why should I go for Aadhar card when I have several ids including passport...have we not lived with ration card as if all these years? Govt is getting rotten day by day, making avenues for fresh corruption to happen. Has the bill been passed by parliament on UID as yet? Important concern is UID is going to destroy the ape old public distribution system.

from: Bhargavi

Posted on: Nov 24, 2011 at 19:09 IST

Dear Sirs, I think the government can introduce another rule to produce your Aadhaar card even to get your monthly salary from your employer!. Can we destroy our Ration cards after receiving the Aadhaar cards? as nowadays one cannot afford to maintain TWO Wives. Krishnamoorthy

from: Krishnamoorthy S

Posted on: Nov 26, 2011 at 12:06 IST

there is no point in making it mandatory for lpg issue since many districts in tamilnadu has not been issued with aadhar card/number. can anybody produce a document when the same has not been issued at all.

from: a.mahadevan

Posted on: Dec 7, 2011 at 11:25 IST

Your Name:

email:

Make a comment

1000 characters left

1. Comments will be moderated

4163
462-

2. Comments that are abusive, personal, incendiary or irrelevant cannot be published.
3. Please write complete sentences. Do not type comments in all capital letters, or in all lower case letters, or using abbreviated text (example: u cannot substitute for you, d is not 'the', n is not 'and').
4. We may remove hyperlinks within comments.
5. Please use a genuine email ID and provide your name, to avoid rejection.



464
463

Latest in this section

Memorable Pongal at the Madras Regimental Centre Dream run Itsy bitsy Audio Beat: Krishnaveni Panjaalai
Audio Bear: Kondan Koduthan Two to tango Tunesmith Blast from the Past: Ponvayal 1954 Outtakes: French
Impressionism Cinema Quiz

Most Popular Most Commented

Memorable Pongal at the Madras Regimental Centre Priority for implementation of schemes: Collector Special
buses to clear Pongal rush Passport applications to be processed faster Sudanese students attacked Narain
Karthikeyan lives up to the 'Challenge' A wedding to remember Covai Flower show Burns victim shifted to
private hospital Two girls drown in quarry

Ads by Google

476.
67



Ads by Google

Home for the Aged

All we need is love care and a little time to spare!

spbangalore.com/



Today's Paper

ePaper This Day That Age Crossword Archives Obituary

Group Sites

The Hindu Business Line Sportstar Images Frontline

Printable version | Jan 16, 2012 9:27:13 AM |

<http://www.thehindu.com/news/cities/Coimbatore/article2584445.ece>

© The Hindu



About Us Contacts Archives Subscriptions RSS Feeds Site Map

Home

News

Opinion

Sport

Business

486
485[Arts](#)[Life & Style](#)[S & T](#)[Education](#)[Health](#)[Jobs](#)[Classifieds](#)[Today's Paper](#)[Topics](#)[Group Sites](#)[The Hindu Business Line Sportstar Frontline](#)[Publications eBooks Images](#)

Disclaimer: *The Hindu* is not responsible for the content of external internet sites.

Republication or dissemination of the contents of this screen are expressly prohibited without the written consent of *The Hindu*.

Comments to web.thehindu@thehindu.co.in Copyright © 2012, The Hindu

True Copy
for
Adv

Exh-7

167
15/01/2012
1468

केंद्र शासनाच्या 'आधार' या योजनेतर्गत प्राप्त
करावयाच्या संकेतांकाची सांगड देतनाशी घालण्याबाबत
करावयाची कार्यवाही

महाराष्ट्र शासन,
वित्त विभाग,

तिसरा मजला, मंत्रालय, मुंबई

शासन निर्णय क्रमांक:संकीर्ण-१०११/प्र.क्र.-२६/कोषा-प्र-५

दिनांक १८ एप्रिल २०११

प्रस्तावना :-

राज्य शासकीय कर्मचाऱ्यांचे वेतन आहरण व सवितरण अधिकार्यांनी कोषागारांवर काढलेल्या वेतन देयका आधार
कारण्यात येते. तर इतर निमशासकीय संस्थांच्या कर्मचाऱ्यांच्या वेतनाकरिता देय अनुदान देण्याकरिता कोषागारांवर विहित
नमुन्यातील देयके कोषागारांमध्ये सादर केली जातात. वेतनावर शासनाकडून मोठ्या प्रमाणावर पैसा खर्च होतो. त्यामुळे दुबार /
चुकीची / अवैध स्वरूपाची प्रदाने पांबविण्याकरिता उपाययोजना करणे आवश्यक झाले आहे.

केंद्र शासनाच्या 'आधार' या योजनेतर्गत सर्व नागरीकाना नोंदणी करून संकेतांक प्राप्त करणे अत्यावश्यक आहे.
त्याकरिता केंद्र शासनाने युनिक आयडेंटिफिकेशन ऑथॉरिटी ऑफ इंडिया ह्या संस्थेची निर्मिती केली आहे. राज्य शासकीय कर्मचारी,
जिल्हा परिषद / पंचायत समित्या इत्यादींचे कर्मचारी, मान्यताप्राप्त व अनुदानित शैक्षणिक संस्थांतील कर्मचारी, अकृषी व कृषी
महाविद्यालये, त्यांच्या अधिपत्याखालील संस्था, तसेच सामाजिक न्याय आणि आदिवासी विकास विभागांतर्गत अनुदानित व
मान्यताप्राप्त शैक्षणिक व इतर संस्थांतील कर्मचाऱ्यांची नोंदणी या योजनेतर्गत त्वरीत व्हावी, तसेच या सर्व संस्थांमधील कर्मचाऱ्यांचे
वेतन देयक संगणकीय प्रणालीद्वारे तयार करण्याचे काम ताबडतोबीने सुरू व्हावे तसेच युटायडी संकेतांकाची सांगड देतनाशी घालणे
शक्य व्हावे यासाठी कार्यपध्दती विहित करण्याची बाब शासनाच्या विचाराधीन होती. युआयडी ऑथॉरिटी ऑफ इंडिया, या संस्थेची
राज्यातील संबंधित संस्था, व इतर संबंधितांशी विचार विनिमय केल्यानंतर शासन आता खालील प्रमाणे आदेश देत आहे.

शासन निर्णय

- १) सरदारी योजना राज्य शासकीय कर्मचारी, जिल्हा परिषद / पंचायत समित्या इत्यादींचे कर्मचारी, मान्यताप्राप्त व
अनुदानित शैक्षणिक संस्थांतील कर्मचारी, अकृषी व कृषी विद्यापिठे व त्यांच्या अधिनस्त महाविद्यालये व सामाजिक
न्याय आणि आदिवासी विकास विभागांतर्गत अनुदानित व मान्यताप्राप्त शैक्षणिक व इतर संस्थांतील दांचे कर्मचारी
यांना लागू राहील.
- २) या संदर्भात युआयडी अंतर्गत नोंदणीकरिता सर्व कार्यालयांतील कर्मचाऱ्यांकरिता (शासकीय कर्मचाऱ्यांसह इतर सर्व
प्रकारचे कर्मचारी) वेळापत्रक नेमून देण्यात आले आहे. त्याप्रमाणे संबंधित कार्यालयातील कर्मचाऱ्यांना त्यांच्या
संदर्भातील नमुन्यासह (केवायआर आणि केवायआर+) वेळापत्रकाप्रमाणे ठरवून दिलेल्या युआयडी स्टेशन्सवर
नोंदणीकरिता हजर राहण्याच्या सूचना देण्यात याव्यात. याबाबतची जबाबदारी सोबत जोडलेल्या वेळापत्रकातील
रकाना क्रमांक ७ व ८ मध्ये दर्शविलेल्या संबंधित अधिकार्यांची राहील.
- ३) या योजनेचा पहिला टप्पा २० एप्रिल, २०११ पासून ते ३० जून, २०११ पर्यंत राहील. या टप्प्यात सर्व शासकीय
कर्मचाऱ्यांची नोंदणी करण्यात येईल.
- ४) शासकीय कर्मचाऱ्यांच्या संदर्भात याबाबतची कार्यपध्दती खालील प्रमाणे राहील.

- अ) ज्या शासकीय कार्यालयातील कार्यालय प्रमुख / आहरण व संचितरण अधिकार्यांनी त्यांच्या अधिनस्त सर्व कर्मचाऱ्यांची नोंदणी "सेवाधर" या प्रणालीवर अद्यापही केलेली नाही त्यांनी दिनांक ३०/०४/२०१९ पर्यंत तशी नोंदणी करणे अनिवार्य आहे. सर्व विभागांच्या विभाग प्रमुखांनी ही गाब त्यांच्या अधिनस्त सर्व कार्यालयांच्या निदर्शनास आणून, याबाबत विहित कालमर्यादेत कार्यवाही होईल याची दक्षता घ्यावी.
- ब) ज्या कार्यालयांची सेवाधर मधील नोंदणी पूर्ण झाली आहे त्यांनी कर्मचाऱ्यांची माहिती दर्शविणाऱ्या विहित नमुन्यातील माहिती सेवाधरमध्ये उपलब्ध करून दिलेल्या सुविधेच्या आधारे तयार करून त्याच्या प्रती मुद्रीत करून घ्याव्यात. आहरण व संचितरण अधिकार्यांनी त्यावर स्वसही करावी व सदर नमुना युआयडी स्टेशनवरील ऑपिकर्यांचे प्रतिनिधी यांना द्यावा व कर्मचार्यांना नेमून दिलेल्या कालावधीत युआयडी स्टेशनवर नोंदणीकरिता पाठवावे.
- क) कर्मचार्यांनी युआयडी संबंधीत दोन नमुने (केवळ आर आणि केवळ आर+) संपूर्ण माहिती भरून नोंदणीसाठी येतांना सोबत आणावे. हे दोनही नमुने कर्मचार्यांनी युआयडी स्टेशनवर नोंदणी करणाऱ्या कर्मचार्यांना द्यावे.
- ड) युआयडी प्राविष्टरणाने निर्दिष्ट केलेल्या अभिकर्त्यांचे प्रतिनिधी युआयडी स्टेशनवरील संपणकार्य या नमुन्यातील माहिती भरतील, तसेच संबंधित कर्मचार्यांच्या डोळ्यांचा (Iris) छायाचित्र घेतील. त्याच प्रमाणे कर्मचार्यांच्या दोन्ही हातांच्या इंग्रही बोट्यांचे ०२ आणि कर्मचार्यांचे छायाचित्र यांची नोंद स्टेशनवरील दंडावर केली जाईल.
- फ) शासकीय कर्मचार्यांनी उपरोक्त प्रमाणे नोंदणी पूर्ण झाल्यानंतर प्राप्त तेजाच्या पोचपावती वरील नोंदणी कर्मांक (Enrollment Number) वर "न" येथे नमूद केलेल्या सेवाधरमधील मुद्रीत नमुन्यात त्यांच्या नावासोबत नमूद करावा व निमोडीत स्थापरी करावी. सर्व कर्मचार्यांची नोंदणी पूर्ण झाल्यानंतर सदर नमुन्यातील माहिती आधारे आहरण व संचितरण अधिकार्यांनी नोंदणी कर्मांकची नोंद सेवाधरमध्ये करावी. तसेच ज्यावेळी युआयडी कर्मांक प्राप्त होईल त्यावेळी त्याचीही नोंद संबंधित कर्मचार्यांच्या नावापुढे सेवाधरमध्ये करावी.
- ग) याकरिता लागणारे केवळ आर, केवळ आर+ हे नमुने युआयडी प्राविष्टरणकडून उपलब्ध करून दिले जातील व ते अधिदान व सेवा कार्यालय, मुंबई, कोबागार कार्यालये, उपकोबागार कार्यालये तसेच जेथे उपकोबागार कार्यालये उपलब्ध नाहीत तेथे सहसिलदार कार्यालयांमध्ये प्राप्त होतील.
- घ) सोबत जोडलेल्या वेळापत्रकातील रकाना क्रमांक ४ व ७ मध्ये दर्शिलेले अधिकारी उपरोक्त कार्य पध्दतीच्या यशस्वी अंमलबजावणीकरिता जबाबदार राहतील.
- ५) या कामाकरिता प्रत्येक स्तोबागार / उपकोबागार / तहसिल कार्यालय येथे त्या संबंधित कार्यालयांनी एका कर्मचार्याची नियुक्ती उपलब्ध कार्याधीन ठेवून विशेष करून करावी.
- ६) दुसऱ्या टप्प्यात शिल्लक परिषद व पांचायत समिती यांमधील कर्मचार्यांचा तसेच जिल्हा परिषदेच्या अखत्यारीतील शाळांमधील कर्मचार्यांची नोंदणी पाहण्यात येईल.
- ७) तिसऱ्या टप्प्यात प्राथमिक, माध्यमिक, उच्च व तंत्र शिक्षण मान्यताप्राप्त व अनुदानित शैक्षणिक संस्थांमधील कर्मचार्यांची नोंदणी घेईल. चौथ्या टप्प्यात ग्रामपंचायत स्तरावरील कर्मचारी, तर पाचव्या

166
176

टप्प्यात सामाजिक न्याय तसेच आदिवासी विकास विभागाच्या अखत्यारीतील मान्यताप्राप्त व अनुदानित संस्थेतील कर्मचाऱ्यांची नोंदणी केली जाईल.

पहिल्या टप्प्यातील कामाचा वेग पाहून तिसऱ्या टप्प्यापासून पुढील टप्प्यातील कार्यवाही दुसऱ्या टप्प्यासोबत करता येईल काय याबाबत वित्त विभाग आणि माहिती तंत्रज्ञान विभाग चर्चा करून निर्णय घेतील.

८) शासकीय कर्मचाऱ्यांव्यतिरिक्त इतर संस्थांच्या कर्मचाऱ्यां संदर्भात याबाबतची कार्यपद्धती खालील प्रमाणे राहिल.

अ) दुसऱ्या टप्प्यापासून समाविष्ट असलेल्या संस्थांच्या अखत्यारीतील सोबत जोडलेल्या वेळापत्रकातील रकाना क्रमांक ४ येथे दर्शविलेल्या आहरण व सवितरण अधिकाऱ्यांनी या शासन निर्णयासोबत जोडलेल्या नमुन्यातील त्यांच्या आणि / किंवा त्यांच्या अधिनस्त कार्यालयाची संबंधित माहिती भरून त्यावर स्वाक्षरी करावी व ते नमुने वेळापत्रकातील रकाना क्रमांक ९ मध्ये दर्शविलेल्या ठिकाणी उभारण्यात यावयाच्या युआयडी स्टेशनवरील युआयडी प्राधिकरणाने नेमलेल्या अधिकार्यांच्या प्रतिनिधीकडे रकाना क्रमांक ३ मध्ये दर्शविलेल्या कालमर्यादेत आणि आखून दिलेल्या वेळापत्रकाप्रमाणे न चुकता सुपूर्द करावी.

ब) कर्मचाऱ्यांना नेमून दिलेल्या झालावधीत (सोबत जोडलेल्या वेळापत्रकातील रकाना क्रमांक ५) युआयडी स्टेशनवर नोंदणीकरिता पठवावे.

ड) कर्मचाऱ्यांनी युआयडी संदर्भित दोन नमुने (केवायआर आणि केवायआर+) संपूर्ण माहिती भरून नोंदणीसाठी येताना सोधत आणावे. हे दोनही नमुने कर्मचाऱ्यांनी युआयडी स्टेशनवर नोंदणी करणाऱ्या कर्मचाऱ्यांना हावे.

इ) युआयडी प्राधिकरणाने निश्चित केलेल्या अभिकर्त्यांचे प्रतिनिधी युआयडी स्टेशनवरील संगणकावर या दोनही नमुन्यातील माहिती भरतील, तसेच संबंधित कर्मचाऱ्यांच्या डोळ्यांचे (Iris) छायाचित्र घेतील. त्याच प्रमाणे कर्मचाऱ्यांच्या दोन्ही हातांच्या दहाही बोटांचे तसे आणि कर्मचाऱ्यांचे छायाचित्र यांची नोंद स्टेशनवरील यंत्रादर केली जाईल.

ई) कर्मचाऱ्यांनी उपरोक्त प्रमाणे नोंदणी पूर्ण झाल्यानंतर प्राप्त होणाऱ्या पोचपावती वरील नोंदणी क्रमांक (Enrollment Number) वर "अ" येथे नेमून केलेल्या नमुन्यात त्यांच्या नमुनेसमोर नेमून करावा. व दिनांकीत स्वाक्षरी करावी. सर्व कर्मचाऱ्यांची नोंदणी पूर्ण झाल्यानंतर सदर नमुने संबंधित कोषागार / उपकोषागारातील या संदर्भातील समन्वय अधिकाऱ्याच्या सुपूर्द करावे. यातील माहिती आधारे नोंदणी क्रमांदाची नोंद संगणकामध्ये करण्यात येईल. तसेच ज्यावेळी युआयडी क्रमांक प्राप्त होईल त्यावेळी त्याचीही नोंद संबंधित कर्मचाऱ्यांच्या नांवापुढे संगणकात करण्यात येईल.

फ) याकरिता सागणारे केवायआर, केवायआर+, हे नमुने युआयडी प्राधिकरणाकडून उपलब्ध करून दिले जातील व ते अधिदान व लेखा कार्यालय, मुंबई, कोषागार कार्यालये, उपकोषागार कार्यालये तसेच जेथे उपकोषागार कार्यालये उपलब्ध नाहीत तेथे तहसिलदार कार्यालयांमध्ये तसेच इतर नेमून घावयाच्या ठिकाणी प्राप्त होतील.

घ) सोबत जोडलेल्या वेळापत्रकातील रकाना क्रमांक ४, ७ व ८ मध्ये दर्शविलेले अधिकारी उपरोक्त कार्य पद्धतीच्या यशस्वी अंमलबजावणीकरिता जबाबदार राहतील.

९) राज्य शासनाच्या युआयडी प्राधिकरणाने राज्यातील प्रहसूल विभागीयस्तरावरील कोषागारांमध्ये प्रत्येकी चार, उर्वरित कोषागारांमध्ये प्रत्येकी दोन, प्रत्येक उपकोषागारामध्ये प्रत्येकी एक, ज्या तालुक्याच्या ठिकाणी उपकोषागार उपलब्ध

नाही अशा तात्तुकात : हरित कार्यालयात प्रत्येकी एक आणि मुंबईतील ३ विधान व लेखा कार्यालय, बॉम्बे येथे पांच आणि फोर्ट येथे दोन : शाखाणे स्वतःच उपभरणयत यावेत. तसेच या प्रत्येक ठिकाणी आवश्यक तेवढी नोंदणी यंत्रे उपलब्ध करून देण्यात वत युआयडी प्राधिकरणाने त्यांनी नेमलेल्या अधिकार्यांना आदेश द्यावेत.

१०) शासकीय कर्मचाऱ्यांची नोंदणी वेळापत्रकाप्रमाणे पूर्ण झाल्याबरोबर अथवा तत्पूर्वी शक्य होईल त्याप्रमाणे दर ८ सध्या नेमूद केलेल्या स्टेशनरीस येथे दुपारच्या टप्प्यातील इतर कर्मचाऱ्यांच्या नोंदणीकरिता वेळापत्रकातील रकाना क्रमांक ९ मध्ये दर्शविलेल्या रंगभट्टा ठिकाणी भरून त्या ठिकाणी नोंदणीचे काम सुरू करण्याबाबत युआयडी प्राधिकरणाने त्यांनी नेमलेल्या अधिकार्यांना आदेश द्यावेत.

११) कर्मचाऱ्यांना नोंदणीबिरता उपरोक्त प्रमाणे नेमून दिलेल्या स्टेशनरी ऐवजी त्यांच्या घराजवळ उपलब्ध असणाऱ्या युआयडी स्टेशनरीस वापराची मुदत तयार केल्या जाईल. असे वेळ्यास त्यांनी यांना प्राप्त होणाऱ्या तात्पुरत्या क्रमांकाची (Enrollment Identification Number) महिती आणि पोचपावतीची प्रत त्यांच्या आहरण व सवितरण अधिकार्यांना (रक्षण क्रमांक ७) दिली अधिकारी) न घुक्ता द्यावी.

१२) दर अनुक्रमांक १ मध्ये नेमूद केलेल्या संस्थांमधील सर्व कर्मचाऱ्यांची या योजनेत नोंदणी आखून दिलेल्या वेळापत्रकातील तारखेपर्यंत पूर्ण करण्यात यावी. अशी नोंदणी करत असतांनाच संबंधित कर्मचाऱ्यांचे वेतन संगणकीकृत प्रणालीत कोठ्यावर नोंदणी करिता महिती संगणकीय प्रणालीवर भरली जाणार आहे. त्यामुळे वेळापत्रकात दर्शविलेल्या महिन्याचे वेतन देयक शक्यतो सदर प्रणालीच्या आधारे तयार करण्यात यावे.

१३) अशा प्रकारे देयक संगणक प्रणालीच्या आधारे तयार करणे शक्य न झाल्यास अथवा या योजनेखालील कर्मचाऱ्यांची नोंदणी विहित मुदतीत पूर्ण होऊ न शकल्यास, आहरण व सवितरण अधिकार्यांनी या शासन निर्णयासोबत जोडलेल्या नमुना-१ मधील माहिती भरून व ती प्रमाणीत / स्वाक्षरीत करून तो नमुना त्यांच्या नेमून दिलेल्या महिन्याच्या वेतन देयकासोबत जोडावा. अशा प्रकारे नमुना-१ मधील प्रमाणपत्र देयकासोबत जोडले नसल्यास वेतन देयक कोणावर नोंदणी करिता येईल याबाबत जाणार नाही. जिल्हा परिक्षां तसेच टपोरेत क्रमांक-३ मध्ये नेमूद केलेल्या इतर संस्थांनी त्यांच्या कर्मचाऱ्यांच्या वेतनाबद्दल त्यांना कोणावर नोंदणी प्राप्त होणाऱ्या सहाय्यक अनुदानाच्या देयकासोबत असे प्रमाणपत्र जोडावे.

१४) या योजनेकरिता सांगणारे सर्व प्रकारचे तांत्रिक सहाय्य, आशावादी विकासकरिता सांगणारी तांत्रिक मदत व पुरेसा कर्मचारी वर्ग माहिती तंत्रज्ञान विभागाने उपलब्ध करून द्यावा.

१५) राज्यातील युआयडी प्राधिकरणांना आवश्यक तेवढी यंत्रे तसेच मनुष्यबळ उपलब्ध करून द्यावे. त्याचप्रमाणे या प्रकल्पाकरिता सांगणारे सर्व प्रकारचे तांत्रिक सहाय्य सुद्धा उपलब्ध करून द्यावे.

१६) या योजनेची यशस्वी अंमलबजावणी करण्याकरिता जिल्हा परिषदांचे मुख्य लेखा व वित्त अधिकारी / शालेय शिक्षण संचालक (प्राथमिक व माध्यमिक) / शिक्षण संचालक (उच्च शिक्षण, तांत्रिक शिक्षण, व्यवसाय शिक्षण, इत्यादी) / कृषी संचालक / फर्मोल्परेशन संचालक तसेच वेतनाकरिता शासनाकडून सहाय्यक अनुदान कोषागारामार्फत आहरित करणाऱ्या सर्व संबंधित आहरण व सवितरण अधिकारी यांना जबाबदार धरण्यात येईल.

१७) राज्यातील सर्व विभागीय आयुक्त, सर्व जिल्हाधिकारी, जिल्हा परिषदांचे मुख्य कार्यकारी अधिकारी यांनी या प्रकल्पाला आवश्यक ती सर्व गरजा कटावी व नेमून दिलेली जबाबदारी पार पाडावी.

471

20990892948433001

471

(2) सदर शासन निर्णय राज्य शासनाच्या संकेत स्थळावर प्रसिध्द करण्यात आला असून त्याचा संकेतांक -

असा आहे.

महाराष्ट्राचे राज्यपाल यांचे आदेशान्वये तथा नावाने



(राजेश अरव्हिंद)

सचिव (लेखा व कोषागारे)

महाराष्ट्र शासन, वित्त विभाग

प्रति,

राज्यातील सचिव

मुख्यामंत्र्यांचे व उप मुख्यामंत्र्यांचे सचिव,

जवळ मंत्री व राज्यमंत्री यांचे खाजगी सचिव,

सर्व मंत्रालयीन प्रशासकीय विभाग,

प्रशासकीय विभागाच्या नियंत्रणाखालील सर्व कार्यालय पत्रे,

महोत्तेजापाल (लेखा व अनुश्रुत्या) - १, महाराष्ट्र, मुंबई

महोत्तेजापाल (लेखा व अनुश्रुत्या) - २, महाराष्ट्र, नागपूर

महोत्तेजापाल (लेखा परीक्षा) - १, महाराष्ट्र, मुंबई

महोत्तेजापाल (लेखा परीक्षा) - २, महाराष्ट्र, मुंबई

महोत्तेजापाल (वर्गनिष्पत्ती लेखापरीक्षा), महाराष्ट्र, मुंबई

उप महासंचालक, UIDAI, पश्चिम विभाग, मुंबई

प्रधान सचिव, महाराष्ट्र विधानमंडळ, सचिवालय, मुंबई

सर्व विभागीय आयुक्ता,

सर्व निहाळीधिकारी,

सर्व निलदा पारबदांचे मुख्य कार्यकारी अधिकारी,

प्रबंधक, उच्च न्यायालय (मूळ शाखा), मुंबई,

प्रबंधक, उच्च न्यायालय (अपीन शाखा), मुंबई,

प्रबंधक, महाराष्ट्र प्रशासकीय व्यापारिकरण, मुंबई,

प्रबंधक, लोक आयुक्त व उप लोक आयुक्त यांचे कार्यालय,

मुंबई,

सचिव, महाराष्ट्र लोकसेवा आयोग, मुंबई,

संचालक, लेखा व कोषागारे, महाराष्ट्र राज्य, मुंबई,

मुख्य लेखा परीक्षक, स्थानिक निधी लेखा, कोकण भवन,

नवी मुंबई

सह संचालक, लेखा व कोषागारे, पुणे / नशिक /

औरंगाबाद / अमरावती / नागपूर / कोकण भवन, नवी

मुंबई.

अधीक्षक व लेखा अधिकारी, मुंबई / वांद्रे,

निवासी लेखा परीक्षा अधिकारी, मुंबई,

सर्व कोषागार अधिकारी,

सर्व उप कोषागार अधिकारी,

निवड रस्ती, वित्त विभाग - कोषा प्र - ५.

25

[illegible]

| अ. | क. | १. | २. | ३. | ४. | ५. | ६. | ७. | ८. | ९. |
|----|--|---|---|---------------------------------------|---|---|---|---|---|---|
| | संस्थानिहाय कर्मचारी प्रकार | कायलवा बरेलची माहिती विहित नमुन्यात सादर करण्याकरिता मुदत | जबाबदार अधिकारी करवावाकरिता नमुन्यात सादर माहिती विहित करण्याकरिता मुदत | युआयडी नोंदणी करिता नोंदणी करिता मुदत | रत्ना इत्यादी कारवाईमुळे नोंदणी न होऊ शकते-या कारवाईमुळे मुदत | वृद्ध व/अंधांमार्फत माहिती विहित नमुन्यात भरणे कार्यवाहीत आणणे मुदत | अधिकारी | भा प्रकल्पाच्या प्रगती अंमलबजावणीसाठी अबाबदार अधिकारी | युआयडी नोंदणीकरिता नमुन्यात भरणे मुदत | |
| ३) | सामाजिक न्याय / आदिवासी विकास विभागाच्या अखत्यारीतील विभागाप्रधान व अग्रणीत संस्थातील कर्मचारी | दिनांक ३१/०५/२०११ | समाल कल्याण / अप्र आर्यून आदिवासी विकास अप्र आर्यून | दिनांक ०१/०८/२०११ ते ३०/०९/२०११ | समाल कल्याण / अप्र आर्यून आदिवासी विकास | दिनांक ३१/०८/२०११ ते ३०/०९/२०११ | समाल कल्याण / अप्र आर्यून आदिवासी विकास | समाल कल्याण / अप्र आर्यून आदिवासी विकास / संस्थित समाल कल्याण / अप्र आर्यून आदिवासी विकास | समाल कल्याण / अप्र आर्यून आदिवासी विकास / अप्र आर्यून (वर्ग-१) / अप्र आर्यून (वर्ग-२) / अप्र आर्यून | समाल कल्याण / अप्र आर्यून आदिवासी विकास |

टिप :- पहिल्या टप्प्यातील कामाचा वेग पाहून ३ ते ६ या टप्प्यातील काढवाही दुसऱ्या टप्प्यासोबत करतो घेईल त्या याबाबत नित निष्पण आणि माहिती तंत्रज्ञान विभाग वर्वी करून निराप घेतील.

472
473

474
475

युवावधी येतुन संगठ
(तेवार्पवत पूर्ण आरुन अंगरतः शाली परतोरती आहे अशा आडरण व संवितरण ऽ विकासांसाठी)

कोषागार संकेतांक (चार अंकी)

कोषागाराचे नांव

आडरण व संवितरण अधिकारी संकेतांक
(सहा अंकी)

आडरण व संवितरण अधिका याचे
पत्तनाम

गोजागार सपडिगत

योजना संकेतांक (आठ अंकी)

योजनाचे नांव

| अ.क्र. | कर्मचार्याचे नांव (उजवत उतरत हा) | सेवाचे ग. र. (रा.क. १९ अंकी) | नोकरी करणक (इंग्रजी- १८ अंकी) | कर्मचार्याची शिनाकरी स्वासरी |
|--------|----------------------------------|------------------------------|-------------------------------|---------------------------------|
| १ | | | | |
| २ | | | | |
| ३ | | | | |
| ४ | | | | |
| ५ | | | | |
| ६ | | | | |
| ७ | | | | |

| आडरण व संवितरण अधिकारी | |
|---|--|
| नांव | |
| सही | |
| दूरध्वनी क्रमांक / भ्रम (ध्वनी क्रमांक) | |

योजना समेकांक (आठ अंकी)

योजनेचा तपशिल

योगजेंचे नाव

(जास्त कर्मचाऱ्यांची माहिती भरण्याकालिता)

| | |
|-------------------------------------|--|
| आहरण य संवितरण अपिकारी | |
| नाव | |
| सही | |
| दरखती क्रमांक / प्रमाणपत्री क्रमांक | |

9th
~~5th~~

| | |
|----------------|--------------------------|
| | 2014 2015 / 2016 2017 |
| | 2018 |
| | 2019 |
| 2020 2021 2022 | |

| | | |
|--------------------------------|-------|------|
| কালিদাস মন্ডল (Head of Office) | তারিখ | |
| | ১৯৭৭ | |
| | ১৯৭৭ | ১৯৭৭ |
| | ১৯৭৭ | ১৯৭৭ |

[illegible]

১৯৬৮-৬৯

የቤተ ክርስቲያን

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

(1942 Etc) 1942-1943

የጊዜ ልዩነት

(12/2/1912) 12/2/1912 12/2/1912 12/2/1912

~~96/7.~~
66h

178
177

(एका पेजा जास्त योजना संकेतांक असल्यात। गवीन योजना संकेतांकरास खालील कर्मधन्याची माहिती भरण्याकरिता)

योजनाचा तपशिल

योजना संकेतांक (आठ अंकी)

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

योजनाचे नाव

| |
|--|
| |
|--|

कर्मधन्यांचा तपशिल

| अ.क्र. | कर्मधन्याचे नाव (ठळक अक्षरात) | जन्म र्माण (दिदि/मा/वसव) | लिंग (स्त्री / पुरुष) | नवीणी क्र. रंक (ईआयडो- २८ अंकी) | कर्मधन्याची दिनांकीत स्वाकरी |
|--------|-------------------------------|--------------------------|-----------------------|---------------------------------|------------------------------|
| १ | | | | | |
| २ | | | | | |
| ३ | | | | | |
| ४ | | | | | |
| ५ | | | | | |
| ६ | | | | | |
| ७ | | | | | |
| ८ | | | | | |

कार्यालय प्रमुख (Head of Office)

| | |
|-------------------------------------|--|
| नाव | |
| सही | |
| दूरध्वनी क्रमांक / भवणध्वनी क्रमांक | |

आडरण व संचितरण अधिकारी

| | |
|--------------------------------------|--|
| नाव | |
| सही | |
| दूरध्वनी क्रमांक / संचणध्वनी क्रमांक | |

UID PAYROLL LINKAGE

(For DDOs who have entered full/partial data in Sevaarth)

Treasury Code (4 Digits)

Treasury Name

DDO Code (6 Digits)

DDO Designation

Scheme Details

Scheme Code
(8 - Digits)

Scheme Description

Employee Details

| S. No | Name of Employee (BLOCK LETTERS) | Sevaarth Code (11-Digits) | Enrollment Number (EID) (28 Digits) | Dated Signature of Employee |
|-------|-------------------------------------|------------------------------|--|-----------------------------------|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |

| DDO | |
|-----------|--|
| Name | |
| Signature | |
| Telephone | |

~~177~~
180

| |
|----|
| S. |
| No |

UID PAYROLL LINKAGE

(For DDOs who are not on Sevaarth)

480
481

| | | | |
|----------------------|----------------------|--------------------------|----------------------|
| DDO Code (10 Digits) | <input type="text"/> | Treasury Name | <input type="text"/> |
| Sub Office Name | <input type="text"/> | Sub Office Telephone No. | <input type="text"/> |
| Sub Office Address | <input type="text"/> | | |

Scheme Details

| | | | |
|--------------------------|----------------------|--------------------|----------------------|
| Scheme Code (8 - Digits) | <input type="text"/> | Scheme Description | <input type="text"/> |
|--------------------------|----------------------|--------------------|----------------------|

Employee Details

| S. No | Name of Employee (BLOCK LETTERS) | Date of Birth (DD/MM/YYYY) | Gender (Male / Female) | Enrollment Number (EID) (28-Digits) | Dated Signature of Employee |
|-------|----------------------------------|----------------------------|------------------------|-------------------------------------|-----------------------------|
| 1 | | | | <input type="text"/> | |
| 2 | | | | <input type="text"/> | |
| 3 | | | | <input type="text"/> | |
| 4 | | | | <input type="text"/> | |
| 5 | | | | <input type="text"/> | |
| 6 | | | | <input type="text"/> | |

| Head of Office | | DDO | |
|----------------|----------------------|-----------|----------------------|
| Name | <input type="text"/> | Name | <input type="text"/> |
| Signature | <input type="text"/> | Signature | <input type="text"/> |
| Telephone | <input type="text"/> | Telephone | <input type="text"/> |

481 482

(For new employees, use this page)

Scheme Details

Scheme Code
(8 - Digits)

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

Scheme
Description

| |
|--|
| |
|--|

Employee Details

| S. No | Name of Employee (BLOCK LETTERS) | Date of Birth (DD/MM/YYYY) | Gender (Male / Female) | Enrollment Number (EID) (28-Digits) | Dated Signature of Employee |
|-------|-------------------------------------|-------------------------------|---------------------------|--|--------------------------------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Head of Office | | DDO | |
|----------------|--|-----------|--|
| Name | | Name | |
| Signature | | Signature | |
| Telephone | | Telephone | |

(To be used in case DDO draws salary for employees under more than one scheme)

Scheme Details

Scheme Code
(8 - Digits)

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

Scheme
Description

| |
|--|
| |
|--|

Employee Details

| S. No | Name of Employee (BLOCK LETTERS) | Date of Birth (DD/MM/YYYY) | Gender (Male / Female) | Enrollment Number (EID) (28-Digits) | Dated Signature of Employee | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|-------------------------------------|-------------------------------|---------------------------|--|--------------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| 1 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | | | | <table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Head of Office | | DDO | |
|----------------|--|-----------|--|
| Name | | Name | |
| Signature | | Signature | |
| Telephone | | Telephone | |

483

484

नमुना क्रमांक-एक

युआयडी नोंदणी कार्यसूची मासिकाली नोंदी झालेल्या व न झालेल्या कर्मचाऱ्यांची संख्या व शिफारस तक्ता
(जून, २०१९ पासून प्रत्येक महिन्याच्या वेतन घेयकासोबत जोडण्यात यावा.)

प्रशासकीय विभागाचे नांव :-

कार्यालयाचे नांव :-

ठिकाण :-

| अ.क्र. | युआयडी नोंदणी झालेल्या कर्मचाऱ्यांची संख्या | युआयडी नोंदणी न झालेल्या कर्मचाऱ्यांची संख्या | एकूण कर्मचाऱ्यांची संख्या |
|--------|--|--|------------------------------|
| | | | |

प्रमाणित करण्यात आले की, वर नोंदविलेली माहिती योग्य व अचूक आहे.

आहरण व संवितरण अधिकारी

कार्यालय प्रमुख

टिप :- कोषागाराकडे वेतन देयक अथवा वेतनाकरिता मागणी करणाऱ्या अनुदानाच्या प्रत्येक देयकासोबत उपरोक्त नमुना जिल्हा परिषद / शिक्षणाधिकारी / उच्च शिक्षण संचालक / समाज कल्याण अधिकारी इत्यादी सर्व संस्थांच्या आहरण व संवितरण अधिकाऱ्यांनी जोडणे अत्यावश्यक आहे.

True Copy
Adv

L185
4867

IN THE HIGH COURT OF JUDICATURE AT BOMBAY

ORDINARY ORIGINAL CIVIL JURISDICTION

PUBLIC INTEREST LITIGATION NO. OF 2012

Vickram Crishna & Ors

....Petitioners

Versus

Unique Identification Authority of India & Ors....

Respondents

AFFIDAVIT IN SUPPORT

I, Vickram Crishna, the Petitioner No 1 above named;
residing at A-31, Queens Apts, Pali Hill, Bandra, Mumbai- 400 050
do hereby state on solemn affirmation as under:

1. I say that I have filed the above Petition for the reliefs more
specifically set out in the Petition.

2. I repeat, reiterate and adopt each and every statement in the Petition
as if the same were set out herein and form a part of this affidavit.

I crave leave to refer and rely upon the Petition.

3. I say that if the ad-interim reliefs are not granted, grave loss, harm,
injury and prejudice will be caused to the Petitioner and if granted,
no loss, harm, injury and prejudice will be caused to the Respondents.

CANCELLED

86
185

4. I, therefore, pray that the Petition be made absolute with costs
and ad-interim reliefs may be granted.

Solemnly affirmed at Bombay

Dated this 16th day of January, 2012

Identified by me

Mihir Desai
MIHIR DESAI

Advocate for Petitioners

(Signature)

) Petitioner No 1

Bef-8
16/01/2012
D. B. SHINDE
JUDGE
COURT OF SESSIONS
BOMBAY

Before me

16-1-12

IN THE HIGH COURT OF JUDICATURE AT BOMBAY

ORDINARY ORIGINAL CIVIL JURISDICTION

PUBLIC INTEREST LITIGATION NO.

OF 2012

Vickram Crishna & Ors

....Petitioners

Versus

Unique Identification Authority of India & Ors....

Respondents

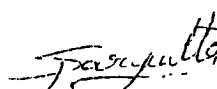
To,
The Prothonotary & Senior Master
High Court, O.O.C.J
Mumbai.

Madam,

ADVOCATE'S CERTIFICATE

I, MIHIR DESAI Advocate for the Petitioner do hereby certify that the present Writ Petition is required to be place before the Division Bench as per the amended Rule 636 (I) (b) of the Bombay High Court, O.S Rules. Therefore the Writ Petition is required to be placed before the Division Bench.

Dated this day of January 2012


Advocate for the Petitioners

