INDEX

VOLUME – I

SL. NO.	PARTICULARS	PAGE(S)
1.	Listing Proforma	A – A2
2.	Synopsis with List of Dates	B – S
3.	Civil Writ Petition with Affidavit	1 – 42
4.	**ANNEXURE –P/1(COLLY):** Summary of Petitioner No. 1's professional work and a copy of the article dated 06.02.2013 published in "The Hindu"	43 - 48
5.	**ANNEXURE – P/2 (COLLY):** Copy of the list of organizations exempted from the purview of Right to Information Act, 2005	49 - 54
6.	**ANNEXURE – P/3:** Copy of media report dated 30.06.2013 with respect to Respondent No.2 promoting the use of AADHAAR number with embassies and missions	55
9.	**ANNEXURE – P/4(COLLY):** (a) Copy of order dated 20.12.2012 passed by the Government of NCT of Delhi, Revenue Department, New Delhi.	56 – 58
	(b) Copy of documents evidencing that AADHAAR card has been made mandatory by various State Governments.	59-79
10.	**ANNEXURE – P/5(COLLY):** (a) Copy of media report dated 01.11.2011 referring to the position taken by the Union Home Ministry on the process of using "introducers"	80-81
	(b) Copy of media report dated 16.12.2011 referring to the position taken by the Union Home Ministry on the process of using "introducers"	82-88
	(c) Copy of media report dated 27.01.2012 referring to the position taken by the Union Home Ministry on the process of using "introducers"	89-90
	(d) Copy of media report dated 28.06.2013 referring to the position taken by the Union Home Ministry on the process of using "introducers"	91-93

11. **ANNEXURE – P/6:**
Copy of a media report dated 01.11.2011 on misuse/abuse of the verifier system adopted by Respondent No.2 94

12. **ANNEXURE – P/7:**
Copy of Respondent No.2's notice bearing No. A-11016/07/10-UIDAI inviting applications for the position of a Biometrics Consultant. 95-111

13. **ANNEXURE – P/8:**
Copy of an independent study titled 'Template Aging in Iris Biometrics: Evidence of Increased False Reject Rate in ICE 2006' by Sarah E. Baker, Kevin W. Bowyer, Patrick J. Flynn and P. Jonathon Phillips 112-151

Cont.....2/

A

LISTING PROFORMA

IN THE SUPREME COURT OF INDIA

1.	Nature of the matter	:	Civil
2.	(a) Name (s) of the Petitioner(s)/Appellant(s) (b) E-mail ID	:	Mr. S.G.Vombatkere & Anr.
3.	(a) Name (s) of Respondent (s) (b) E-mail ID	:	Union of India & Ors.
4.	Number of case	:	Civil Writ Petition No. of 2013
5.	(a) Advocate(s) for Petitioner(s) (b) E-mail ID	:	M/s. K.J.JOHN & CO. mail@kjjohnco.in
6.	(a) Advocate(s) for Respondent(s) (b) E-mail ID	:	N.A.
7.	Section dealing with the matter	:	PIL
8.	Date of the Impugned Order/Judgment	:	N.A.
8A.	Name of Hon'ble Judges	:	N.A.
8B.	In Land Acquisition Matters:- i) Notification/Govt. Order No.(u/s 4, 6) dated issued by Centre/State of ii) Exact purpose of acquisition & village involved	:	N.A.
8C.	In Civil Matters:- i) Suit No., Name of Lower Court ii) Date of Judgment	:	N.A.
8D.	In Writ Petitions:- "Catchword" of other similar matters	:	N.A.
8E.	In case of Motor Vehicle Accident Matters:- Vehicle No.	:	N.A.
8F.	In Service Matters i) Relevant Service rule, if any ii) G.O./ Circular/Notification, if applicable or in question	:	N.A. N.A
8G.	In Labour Industrial Disputes Matters: I.D.Reference /Award No. if applicable	:	N.A.
9.	Nature of urgency	:	Interim relief

10.	In case it is a tax matter:-	:	N.A.
	a) Tax amount involved in the matter		N.A.
	b) Whether a reference/ statement of the case was called for or rejected		N.A.
	c) Whether similar tax matters of same parties filed earlier (may be for earlier/ other Assessment Year)?		N.A.
	d) Exemption Notification/ Circular No.		N.A.
11.	Valuation of the matter:	:	N.A.
12.	Classification of the matter (Please fill up the number & name of relevant category with sub category as per the list circulated)	:	N.A.
	No. of Subject Category with full name	:	08 Letter Petition & PIL Matters
	No. of Sub-Category with full name	:	0812 others
13.	Title of the Act involved (Center/State)	:	
14.	(a) Sub-classification (indicate Section/Article of the Statute)		Article 32
	(b) Sub-section involved		
	(c) Title of the Rules involved (Center/State)		
	(d) Sub-classification (indicate Rule/Sub-Rule of the Statute)		
15.	Point of law and question of law raised in the case:	:	N.A.
16.	Whether matter is not to be listed before any Hon'ble Judge? (Mention the name of the Hon'ble Judges)	:	N.A.
17.	Particulars of identical/ similar cases, if any	:	N.A.
	(a) Pending cases		
	(b) Decided cases with citation		
17A.	Was SLP/Appeal / Writ filed against same impugned Judgment/order earlier? (If yes, particulars)	:	N.A.
18.	Whether the Petition is against interlocutory/ final order/decree in the case	:	N.A.
19.	If it is a fresh matter, please state the name of the High Court and the Coram in the Impugned Judgment/order	:	N.A.
20.	If the matter was already listed in this Court	:	N.A.
	(a) When was it listed?		N.A.
	(b) What was the Coram?		
	(c) What was the direction of the Court		

A-2

21.	Whether a date has already been fixed either by Court or on being mentioned, for the hearing of matter, If so, please indicate the date fixed	:	N.A.
22.	Is there a Caveator? If so, whether a notice has been issued to him?	:	N.A.
23.	Whether date entered in the Computer?	:	N.A.
24.	It is a criminal matter, please state:	:	N.A.
	(a) Whether accused has surrendered		N.A.
	(b) Nature of offence, i.e. Convicted under Section with Act.		
	(c) Sentenced awarded:		N.A.
	(d) Sentence already undergone by the accused.		N.A.
24e)	(i) FIR/RC/etc. Date of Registration of FIR etc. Name & Place of the Police Station		N.A.
	(ii) Name and place of Trial Court Case No. in Trial Court and Date of Judgment		N.A.
	(iii) Name and place of Ist Appellate Court Case No. in Ist Appellate Court and Date of Judgment		N.A.

Date: 02.09.2013

M/s. K.J.JOHN & CO.,
Advocate for the Petitioners,
Code No.1287

B

SYNOPSIS

The present Petition under Article 32 of the Constitution of India is being filed in public interest raising various issues, including among others, protection of fundamental rights under Article 14 and 21 of the Constitution of India.

The core challenge in this petition is the violation of basic human rights as a result of the Unique Identification Project ("UID Project") introduced by the Respondents and which violations will escalate in the future unless checked by this Hon'ble Court.

The 1st Petitioner is a citizen of India is aged about 71 years. The 1st Petitioner is a retired Indian Army officer and is engaged in voluntary social work. In so far as the Unique Identification Project ("UID project") is concerned, the 1st Petitioner has published several articles expressing concerns over privacy and security risks. The 2nd Petitioner is a citizen of India and is also engaged in voluntary social work. He is one of the founders and the National Convenor of the Safai Karmachari Andolan, a human rights organization that has been campaigning for the eradication of manual scavenging and the emancipation of people employed for the purposes of manual scavenging. He was also the convenor of the sub-group on safai karamcharis constituted by the Planning Commission of India. In 2009, he was chosen as the "Ashoka Senior Fellow" of human rights. By virtue of being the founder of Safai Karmachari Andolan, he is also actively involved in a public interest litigation pending before this

C

Hon'ble Court in Writ Petition (civil) No.583 of 2003 Safai Karamchari Andolan and Ors. v. Union of India & Ors. The subject matter of this petition is strict implementation of the Employment of Manual Scavengers and Construction of Dry Latrines (Prohibition) Act, 1993.

The Respondents are implementing a scheme to provide an identification number to residents in India, without regard to whether or not such individuals are Indian citizens. Individuals are being required by the Respondents to part with private biometric information without informing the individual about the consequences of parting with the biometric information, and without the informed consent of the individual.

The biometric information being collected comprises: (i) a facial photograph of the individual; (ii) all ten finger prints; and (iii) a scan of both the iris. The State seeks to create a vast databank containing personal information that can be exploited by the State or private entities against the interest of the citizen/residents and without the knowledge of the citizen/residents. It is plainly ultra vires inasmuch as it is being undertaken:

a. Without any legislative sanction to conduct the exercise;

b. Without any amendment to existing laws relating to citizenship;

c. Without any amendment to the Constitution of India relating to citizenship;

d. Without any statutory guidance or limitation on who can collect the biometric information or how it is to be collected;

e. Without any statutory provision regarding how the biometric information is to be stored and secured throughout the chain beginning with collection of information until the stage of storage;

f. Without any statutory limitation on when the information can be used or by whom it can be used.

The collection of personal biometric information directly impacts the autonomy of an individual and his person. Any exercise on a national scale to secure every individual's biometrics without any legislative safeguards on use, storage, etc. amounts to a direct and nationwide assault on individual freedom.

The project is aimed at persuading public sector as well as private sector service providers to require residents to produce a UID number as a pre-requisite for granting services. It is being represented that unless a person has a UID number, it will become extremely inconvenient for him to access essential services. Illustrative of the coercion employed by different organs of the State are the following notifications/circulars/decisions taken by authorities that now insist upon the AADHAAR number or refuse services:

E

a) The Government of NCT of Delhi, Revenue Department has issued an order on 20-12-2012 making AADHAAR number compulsory for registration of marriages as well as for registration of documents in the Sub Registrar Offices.

b) Similarly, the State of Jharkhand has also made AADHAAR number compulsory for registration of marriages as well as for registration of documents in the Sub Registrar Offices.

c) The State of Karnataka has made AADHAAR number mandatory for availing benefits under government schemes such as social security pensions, LPG connection, ration card etc.

d) The Union Ministry of Petroleum has made AADHAAR number mandatory for 'Direct Benefit Transfer' scheme for LPG customers.

e) In the State of Maharashtra, AADHAAR number has been made mandatory for teaching and non-teaching employees in government aided schools for drawing salary.

f) The State of Kerala has made AADHAAR number mandatory for admission of students in schools and colleges.

F

g) The State of Himachal Pradesh has made AADHAAR number mandatory for admission of students in schools and colleges.

h) The State of Madhya Pradesh has made AADHAAR number mandatory for pension and provident fund.

i) The University Grant Commission has made AADHAAR number mandatory for students applying for scholarship or fellowship. AADHAAR number has been made mandatory by Employees' Provident Fund Organisation.

The Petitioners submit that with each passing day, the Respondents are making AADHAAR card mandatory for all basic rights and services such as education, salary, LPG subsidy, ration card, registration of documents etc. This coercion to enroll for the AADHAAR scheme and collection of sensitive personal data of residents without any safeguard poses a dangerous threat to all residents of the country which may cause irreparable harm to the residents.

It appears that the Respondents are working in coordination with schools to enroll children as well as other persons connected with the schools. It is respectfully submitted that in addition to the points made above, this action is patently illegal inasmuch as children in schools do not have a legal capacity to consent and these children are being yoked to the Aadhaar apparatus for all time.

The UID project and AADHAAR scheme are illegal and violate fundamental rights in the following manner, inter alia:

(i) Ultra Vires: No Legislative Sanction: The Union Government through executive fiat alone and without any legislative safeguard is employing a network of private players to obtain sensitive, personal biometric information of residents in India, including Indian citizens;

(ii) No Informed Consent; This information is being obtained by the State from unsuspecting individuals who are merely seeking a reliable identification (ID) and at the time of obtaining this information, individuals are neither counseled nor informed that there is no statutory protection with regard to the use or misuse of the sensitive personal biometric information they are parting with;

(iii) Private Parties Collecting Information Without Safeguards: The personal sensitive biometric information is not being collected from residents by any statutory authority or government agency and the exercise in the field is being carried out by private entities for profit and these private parties are not subject to any legislative oversight or administrative oversight by any statutory authority;

(iv) Private Dominion Over Biometrics Without Government Control: Personal Security and National Security Issues: The privatization of biometric information of millions of residents which include Indian citizens poses an enormous threat to the autonomy of an individual, his or her

personal liberty and the privacy of the individual and gives dominion and control to private entities over personal information of individuals;

(v) Private Entities : Commercial Largess: Private entities have been allowed to obtain this information from citizens/ residents under the framework of the UID project without UIDAI or the Union Government having regard to the immense commercial worth of the biometric information that is being captured on privately owned computers and databases over which the government has no control or exclusive access;

(vi) Security of Collected Data: In addition to the haphazard and unreliable manner employed by the 2nd Respondent in collecting data, it appears that there is no secure manner in which the 2nd Respondent will store data collected;

(vii) Surveillance : There are several organizations within the government such as the Intelligence Bureau, Research and Analysis Wing (RAW); National Intelligence Grid, Multi Agency Centre and now the Central Monitoring System that operate outside legislative oversight, which organization are exempt from the obligation of disclosure under the Right to Information Act. Upon the UID number use becoming ubiquitous, the Petitioners apprehend that each of these agencies will be able to track individuals on a real time basis increasing the scope of individual

surveillance to a level that is impermissible under the Indian Constitution. Absent any statutory safeguard that prevents access to the information converged through the use of the AADHAAR number, the impugned project and scheme will result in impermissible levels of surveillance in violation of Article 14 and 21 of the Constitution of India;

(viii) Invasion of Privacy: The UID project as conceived and as being implemented will result in an extreme invasion of privacy and a violation of Article 21 in respect of persons who are issued a UID number;

(ix) Undermining Human Dignity : It is submitted that dignity is an important facet of the right to life under Article 21 of the Constitution. The impugned project assaults individual dignity by compelling persons on pain of exclusion from society, to part with biometric information and impinges on dignity by universalizing the requirement of possessing and using an AADHAAR number.

(x) Coercion To Part With Biometrics: The UID number is not being issued only to disadvantaged persons who require some authentic identification before receiving benefits. The project is aimed at persuading public sector as well as private sector service providers to require residents to produce a UID number as an essential requirement for granting services. It is being represented that unless a person has a UID number, it will become extremely

inconvenient for him/her to access essential services. In this manner, individuals are being and will be coerced into parting with their biometrics because otherwise essential services will be withheld from them.

(xi) Failure to Provide an "opt out" Option : The Petitioners submit that in order to pass the test of reasonableness and rationality, any scheme such as the AADHAAR scheme ought to have an option by which an individual may at any time opt out of the system. Quite apart from there being no informed consent when enrolling individuals, the failure to provide such an option violates Article 14 of the Constitution of India and also violates Article 21.

(xii) Flawed Introducer System and Verifier System: The procedure adopted by the Respondent (through private entities) for securing enrolment for AADHAAR numbers includes a drive for enlisting individuals. The process of enrolment for those persons who do not have identification documents and who require to be introduced to the system, involves an agent called the "introducer" who vouches for the enrollee. The 2nd Respondent has laid out criteria for who can act as an introducer. These criteria do not require the "introducer" to know the person he is introducing, thereby compromising the integrity of the entire enrolment process;

K

(xiii) Dismantling of Public Distribution : Although styled as a programme that is designed to help the disadvantaged, in fact the impugned project is likely to cause great harm to this section;

(xiv) Unreliability of Biometrics : The biometrics being collected are an extremely unreliable basis for identifying an individual on a national scale for a country as populous as India. It is an unproven technology which has been abandoned elsewhere in the world; and

(xv) Biometrics Exceptions : Apart from the unreliability of biometrics generally, for certain segments of the population biometrics in the form of finger print and iris scans are not possible to capture because of physical limitations.

The Writ Petition therefore assails the UID Project and AADHAAR scheme on diverse grounds. The frame of the challenge in the present case is wider than those urged in Writ Petition (C) No. 494 of 2012 (Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.) wherein notice was issued by this Hon'ble Court on 30.11.2012.

LIST OF DATES

28.01.2009	The UIDAI is a department of the Union Government functioning within the Planning Commission. UIDAI was notified by the Planning Commission on 28.1.2009.

L

02.07.2009	The Government appointed Shri Nandan M. Nilekani as Chairman of the UIDAI.
September, 2010	The AADHAAR number is a random 12 digit number which is unique for all residents in India. The programme was launched in September, 2010 in rural Maharashtra and had now been extended across India. AADHAAR is intended to be a single source of verification of identity and will link a person's passport number, driving licence, PAN card, voter ID card, bank account address, etc. Although the scheme is touted as being voluntary, as more particularly set out herein, the intent of government is to make it mandatory by aggressively promoting the use of this number amongst service providers. The object is that these service providers will over time insist upon production of the AADHAAR number making it extremely inconvenient to a person not holding a UID number to live and function freely and efficiently in society. Government and the UIDAI are actively requiring personal biometrics to be yielded to databanks in this manner.

M

03.12.2010

Although the programme was launched in September, 2010, the 1st Respondent introduced the National Identification Authority of India Bill, 2010 in Parliament on 3.12.2010. This Bill was referred to the Parliamentary Standing Committee on Finance which tabled its report in Parliament in 13.12.2011. The Committee found that the Bill was wanting in several respects.

The Respondents have not introduced any fresh legislation since then and the project has continued without any legislative framework.

The UIDAI is implementing its project through numerous networks, the most significant of which for the purposes of this petition are the following:

A. Collection network through Registrars and Enrolment Agencies;
B. Technology creation network to implement biometrics identification systems and the storage of information obtained; and
C. Network with government and private agencies to spread the utilization of AADHAAR numbers.

The material facts in respect of each of these structures is described below.

UIDAI does not directly collect any biometric information. It has entered into arrangements with "Registrars". There is no statutory or administrative definition of who qualifies to act as a Registrar. The UIDAI has entered into MOUs with State Governments which require the government to identify departments within government to act as Registrars. This may include departments such as the Consumer Affairs Department or the Civil Supplies Department. The Registrars are allowed to collect such information as they consider necessary even beyond the information required by the UIDAI, depending upon the needs and requirements of the Registrars. However, Registrars themselves do not have the capacity to enroll persons and collect the information. The Registrars, in turn, engage private sector "Enrolment Agencies" who are empanelled with the UIDAI. These enrolment agencies have designated territories where they may conduct their enrolment work.

January, 2011

It appears that out of 220 enrolment agencies, 11 were dis-empanelled by the UIDAI.

Although collected under the banner of the AADHAR project and actively projected as a government exercise no government agency takes responsibility for "cradle to grave" security and safety of the biometric information collected. Specifically, UIDAI takes no responsibility for the security of the personal biometric data being collected. The data is initially collected and stored on computers that do not belong to the UIDAI or the Registrars. The information collected becomes the property of the private individual / private enrolment agencies and can be used by these private parties as they like. There are no effective and enforceable security protocols that ensures that the private enrolment agencies do not misuse the information in their hands. There is no effective and enforceable machinery by which a private enrolment agency can be restrained from duplicating, transmitting or retaining the information obtained through the enrolment

process. UIDAI and the Union Government have both failed and neglected to create a system with technological and legal integrity that would protect the biometric data of millions of Indian citizens and residents which is being collected on private computers. This is a case of ineptitude, negligence and violation of public trust. The state is causing residents and citizens to part with vital personal information without any security framework regarding the protection of this data and this data or any machinery to retrieve data that has fallen into the wrong hands.

Information collected by the enrolment agencies and the data captured is transferred to UIDAI's Central ID Repository (CIDR) via memory sticks through courier services or by directly uploading the data to the CIDR. Each of these methods is fraught with potential leakages and there is absolutely no safety in respect of the data being collected.

The empanelled enrolment agencies comprise private sector companies, trusts, proprietary

concerns / firms, foundations, public limited companies and a range of other entities. The UIDAI does not appear to have empanelled these enrolment agencies on the basis of an established track record of impeccable integrity in preserving and protecting sensitive data. There is no guarantee or assurances regarding what has happened to data already collected and what may happen to data lying with these parties or which may be collected in the future. There is absolutely no screening with regard to the employees of these organizations or their background. There is also no manner in which the UIDAI or the Registrars can check on whether employees of the Registrars and/or the enrolment agencies are misusing the sensitive biometric data which comes under their control. There also does not appear to be any provision either in law or in the contracts entered into by the UIDAI and the enrolment agencies / Registrars with regard to the ownership of the data.

It appears that the UIDAI has entered into arrangements with four consortia to

R

implement the core biometric identification system in support of the AADHAAR Project. These three consortia are entrusted with the task of designing, supplying, commissioning, maintaining and supporting the Biometric Identification System. They are involved in the development of software for enrolment stations, verification of the data and other tasks for validation. The leaders of the three consortia are (i) Accenture; (ii) Mahindra Satyam & Morpho joint venture; and (iii) L1-Identity Solutions.

It also appears that the 2nd Respondent has introduced a new data sharing policy with State Governments for sharing of data collected by it on a request made by the State Government. This 'Data Sharing Policy' records that State Governments expressed reservations about not having access to the information collected under UID Project and to resolve the issue, the 2nd Respondent has agreed to make data available to the State Government for welfare and public services. Although this policy purports to have certain checks and balances, firstly, it strengthens the

apprehension raised by the Petitioners in this petition that the sensitive personal information being collected is capable of being transmitted easily on a request of a party. Secondly, 2nd Respondent is not accountable for such harm as it is not under any legislative control in case of misuse of information. Thirdly, this policy also fails to ensure that the recipient of information does not part with or duplicate the information for its own retention. It is submitted that these ramifications are not explained to persons giving the information under the UID Project and amount to grave violation of right to life and personal liberty.

30.08.2013

It is in the foregoing circumstances that the present Petition under Article 32 of the Constitution of India has been filed by the Petitioners herein seeking to assail the UID project and AADHAAR Scheme on diverse and detailed grounds set out in paragraph 7 of the Petition explaining why the impugned UID project and AADHAAR scheme are ultra vires, illegal null and void.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

CIVIL WRIT PETITION NO. OF 2013

IN THE MATTER OF:

1. Mr. S.G.Vombatkere,
   475, 7th Main Road, Vijayanagar
   1st Stage, Mysore,
   Karnataka – 570 017.

2. Mr. Bezwada Wilson,
   C/o Safai Karamchari Andolan,
   36/13 Ground Floor,
   East Patel Nagar,
   New Delhi-110008. ...Petitioners

Versus

1. Union of India.
   Ministry of Finance,
   North Block,
   New Delhi – 110 001
   Through : The Secretary, Finance

2. Union of India.
   Ministry of Home Affairs,
   North Block Central Secretariat,
   New Delhi - 110 001.
   Though : The Secretary, Home Affairs

3. Unique Identification Authority of India,
   3rd Floor, Tower II,
   Jeevan Bharati Building,
   Connaught Circus,
   New Delhi - 110001.
   Through its Chairman ...Contesting Respondents

A PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA

TO

THE HON'BLE THE CHIEF JUSTICE OF INDIA
AND HIS COMPANION JUSTICES OF THE
HON'BLE SUPREME COURT OF INDIA.

THE HUMBLE PETITION OF THE PETITIONERS ABOVENAMED.

MOST RESPECTFULLY SHEWETH:

1. The 1st Petitioner is a citizen of India is aged about 71 years. The 1st Petitioner is a retired Indian Army officer and is engaged in voluntary social work. In so far as the Unique Identification Project ("UID project") is concerned, the 1st Petitioner has published several articles expressing concerns over privacy and security risks. A resumé of the 1st Petitioner's professional work and a copy of the article is annexed hereto and marked as **ANNEXURE – P/1(COLLY) – (PAGES TO)**.

2. The 2nd Petitioner is a citizen of India and is also engaged in voluntary social work. He is one of the founders and the National Convenor of the Safai Karmachari Andolan, a human rights organization that has been campaigning for the eradication of manual scavenging and the emancipation of people employed for the purposes of manual scavenging. He was also the convenor of the sub-group on safai karamcharis constituted by the Planning Commission of India. In 2009, he was chosen as the "Ashoka Senior Fellow" of human rights. By virtue of being the founder of Safai Karmachari Andolan, he is also actively involved in a public interest litigation pending before this Hon'ble Court in Writ Petition (civil) No.583 of 2003 Safai Karamchari Andolan and Ors. v. Union of India & Ors. The subject matter of this petition is strict implementation of the Employment of Manual Scavengers and Construction of Dry Latrines (Prohibition) Act, 1993.

3. The 1st Respondent is the Ministry of Finance, Union of India, while the 2nd Respondent is the Ministry of Home Affairs, Union of India. The 3rd Respondent is the Unique Identification Authority of India (UIDAI), a non-statutory department of the Union Government operating in the Planning Commission of India. UIDAI is responsible for implementing "AADHAAR" a project that is intended to give a 12 digit unique number to all residents in India, whether citizens or not.

4. The Respondents are amenable to the writ jurisdiction of this Hon'ble Court under Article 32 of the Constitution of India. The Respondents are the "State" within the meaning of Article 12 of the Constitution of India.

THE NATURE OF THE CHALLENGE AND THE ISSUES INVOLVED IN THIS CASE

Fundamental rights violated

5. This petition challenges government actions that violate and threaten to violate the fundamental rights of the Petitioners and other citizens and residents of India. The impugned actions, in particular, violate the Petitioners' fundamental rights guaranteed under Articles 21 and 14 of the Constitution of India.

Public interest litigation

6. This petition is filed as a public interest litigation. The impugned actions, unless prevented, will adversely affect and harm citizens and residents across the country, individually and collectively. The

Petitioners approach this Hon'ble Court bona fide to prevent the violation of basic human rights that have already occurred as a result of the UID Project and which violations will escalate in the future unless checked by this Hon'ble Court.

Core challenge

7. The Respondents are implementing a scheme to provide an identification number to residents in India, without regard to whether or not such individuals are Indian citizens. A central feature of this scheme is that the Respondents through private agencies, without any legal sanction, are collecting personal biometric information including finger prints and a scan of both the iris in the individuals' eyes. This exercise is being conducted without adequate safeguards regarding the process of collecting biometric data. Individuals are being required by the Respondents to part with private biometric information without informing the individual about the consequences of parting with the biometric information, and without the informed consent of the individual. As explained hereafter, the impugned project is ultra vires, illegal and liable to be forthwith struck down / brought to a halt.

8. The UID project and AADHAAR scheme are illegal and violate fundamental rights in the following manner, inter alia:

Ultra Vires: No Legislative Sanction

(A) The Union Government through executive fiat alone and without any legislative safeguard is employing a network of private players to obtain sensitive, personal biometric

information of residents in India, including Indian citizens. The biometric information being collected comprises: (i) a facial photograph of the individual; (ii) all ten finger prints; and (iii) a scan of both the iris.

The exercise of obtaining this information alters fundamentally the relationship between citizen and State. The State seeks to create a vast databank containing personal information that can be exploited by the State or private entities against the interest of the citizen/residents and without the knowledge of the citizen/residents. This exercise has been conceived and is being implemented without any statutory backing. It is plainly ultra vires inasmuch as it is being undertaken:

(i) Without any legislative sanction to conduct the exercise;

(ii) Without any amendment to existing laws relating to citizenship;

(iii) Without any amendment to the Constitution of India relating to citizenship;

(iv) Without any statutory guidance or limitation on who can collect the biometric information or how it is to be collected;

(v) Without any statutory provision regarding how the biometric information is to be stored and secured throughout the chain beginning with acquisition of

biometric data and other demographic information until the stage of storage;

(vi) Without any statutory limitation on when the information can be used or by whom it can be used.

The collection of personal biometric information directly impacts the autonomy of an individual and his/her person. Any exercise on a national scale to secure every individual's biometrics without any legislative safeguards on use, storage, etc. amounts to a direct and nationwide assault on individual freedom. The impugned actions violate Article 21 of the Constitution of India inasmuch as the executive arm of the State is collecting personal biometric information without any sanction of law and in the knowledge that this information can be used against individuals to impinge their liberty.

(B) Reading Part III of the Constitution which enumerates fundamental rights recognized in the Constitution of India, it is evident that all persons in India (citizen and non-citizen) enjoy a number of freedoms and rights in relation to the State. Broadly, these fundamental rights, drawing on other parts of the Constitution, enable persons to preserve and protect their individuality and dignity and guarantee that each person may in the course of his or her life endeavour to attain fulfillment in personal as well as public spheres of activity. The State is prevented by the Constitutional

mandate from interfering in individual pursuits, community pursuits and enterprise of any type except in a manner recognized by the Constitution and provided by law.

The activity of obtaining personal biometric information of an individual cannot be engaged in by the State regardless of whether or not an individual voluntarily gave this information, save and except under a valid law. Having regard to the relationship between individual and State under the Indian Constitution, there is a fetter on the State to act in a manner that would impinge upon the right to life of a person guaranteed under Article 21 and recognized by the Supreme Court in all its dimensions. The constitutional scheme demands that there has to be a legislation to back any action on the part of the State that could potentially impinge on an individual's freedoms. Here, without any legislative backing, the State is collecting sensitive, personal biometric information that potentially may be used for the benefit of the individual or to the detriment of the individual or even not used at all. The moment information of this type is sought to be collected by the State, under the Constitutional scheme there must be legislative backing. Absent any legislative backing, the UID project and the AADHAAR scheme by their very invasive nature are ultra vires and void.

No Informed Consent

(C) This information is being obtained by the State from unsuspecting individuals who are merely seeking a reliable identification (ID). The UIDAI is actively projecting that the biometric information is required for the purpose of issuing a unique identification number to every individual coupled with an identification card. At the time of obtaining this information, individuals are neither counseled nor informed that there is no statutory protection with regard to the use or misuse of the sensitive personal biometric information they are parting with. There is active concealment by the UIDAI of the potential harm that may visit a person from his or her parting with biometric information. This biometric information once obtained by government (and its private collecting agency) can be accessed and used without any protection to the individual and against the individual in criminal investigations and proceedings, in all types of court proceedings, and for a range of governmental activity. Having regard to the porosity of the procedure at present being employed, the information can also fall in the hands of foreign governments and may have already been transmitted to foreign governments clandestinely.

Crucial information that is vital for each individual to retain control over, in order to protect his or her innocence under our criminal justice system, is being collected by the State in advance and stored in a data bank to be available for use at

a future date against the individual. This action of collecting biometric and demographic information by the State without informing individuals regarding its potential use in criminal and other proceedings against the person is destructive of the Rule of Law and violative of Articles 14 and 21 of the Constitution of India.

(D) The biometric and other information of an individual being collected by the Respondents has potentially an enormous commercial value. The personal information of an individual when aggregated with the information of others may be even more commercially valuable. The concerned individuals from whom information is being obtained are not informed about the commercial value of this information and are being required to part with information without payment or knowledge as to the manner which the Respondents may exploit the information for commercial ends. The Petitioners verily believe that the Respondents are fully conscious about the commercial value of the information being collected but are nevertheless not informing persons about its value before securing the information. Indeed, private parties engaged in the business of collecting sensitive personal biometric data of individuals and other data under the Respondents' impugned project and scheme may already be profiting from selling such data behind the back of Respondents.

Private Parties Collecting Information Without Safeguards

(E) The personal sensitive biometric information is not being collected from residents by any statutory authority or government agency. The exercise in the field is being carried out by private entities for profit and these private parties are not subject to any legislative oversight or administrative oversight by any statutory authority. The private entities under private contractual arrangements with UIDAI are projecting that they are an extension of the government machinery and are luring individuals to part with biometric information and other personal data. The private entities are driven purely by a profit motive and their earnings are directly linked to the number of individual enrolments that translate into UID numbers. These private entities do not inform the individuals from whom they obtain the biometric information about the potential harm that may visit the individual in the future from this information becoming available to government agencies, criminal investigators, courts, etc.

More important, the biometric information collected by these private entities (perceived by members of the public as an extension of the government machinery) is in the control of the private entities and can be used / misused by these entities without any government authority learning about the use / misuse. There is no effective data protection law to prevent misuse of biometric data collected under the

impugned project. In other words, vital personal biometric information of residents and others with an enormous potential commercial value is falling into private hands in an unregulated manner with government having no statutory, technological or administrative control over the biometric information. Information that historically and conventionally (if at all) would almost only be available with the government under stringent control is now falling into private hands because of the terribly flawed design of the project. There are no adequate checks and safeguards, to secure this data and the impugned scheme operates to the detriment of residents and for the commercial benefit of unregulated private parties. The impugned action of the State in facilitating and permitting private entities to garner personal biometric information (of immense commercial value) without any technological or other safeguards and without sufficient control over the information is arbitrary, illegal and violative of Articles 14 and 21 of the Constitution of India.

(F) It is submitted that as a matter of Constitutional responsibility and duty there are certain core functions of the State that cannot be delegated to private entities. For example, judging under the criminal justice system cannot be privatized. Likewise, functions and duties discharged by certain Constitutional functionaries such as the Comptroller and Auditor General of India or the Election Commission of

India cannot be discharged by private parties. It is submitted that it is Constitutionally impermissible for the Respondents to permit private parties to secure control or dominion over private sensitive information such as the biometric information of an individual. The Constitution prohibits the State from abdicating its role with regard to protecting the welfare of individuals by allowing private entities to exercise control over an individual's biometric data. Equally, this cannot be done for large segments of society through a drive conducted by private parties to collect this data. Under no circumstances, much less under an unregulated, non-statutory project such as the impugned project can the State cede dominion over personal data that can severely prejudice an individual.

Private Dominion Over Biometrics Without Government Control: Personal Security and National Security Issues

(G) The privatization of biometric information of millions of residents which include Indian citizens poses an enormous threat to the autonomy of an individual, his or her personal liberty and the privacy of the individual. The privatization of this biometric information gives dominion and control to private entities over personal information of individuals. This biometric information can remain in the hands of private entities without the knowledge of any government entity. At a future date, an individual's personal liberty, autonomy and

privacy can be compromised by the private entity parting with this information for commercial gain. Under the UID project and AADHAAR scheme as being implemented, there is no manner of the government ensuring that the biometric information already collected by private entities has not been replicated, copied, sold and / or retained by the private entities for present or future commercial gain.

The privatization of biometric information in the unregulated manner impugned herein poses an enormous threat to national security. There is no Parliamentary or governmental control over the transmission of this personal biometric information by private entities overseas. Crucial personal biometric information of individuals and of vast segments of the people of India can be transmitted overseas to foreign entities and foreign governments, for commercial gain, without the Union Government being aware of the transmission of this information. The information can potentially undermine national security. The biometric information lying in private hands can also pass to a foreign entity upon the Indian entity being purchased by an overseas entity, as there are absolutely no checks or controls in this regard.

At all levels – individual, community and national – the impugned project and actions severely imperil the right to life, safety and security amounting to a transgression of Article 21 of the Constitution of India. The exercise which

has been undertaken by government in a hasty, thoughtless manner without any public discussion or debate; without any Parliamentary discussion or debate; and without so much as a realistic pilot project or study, renders the whole exercise arbitrary, deeply flawed and violative of Article 14 of the Constitution of India.

Private Entities : Commercial Largess

(H) Without prejudice to the submission that the government cannot require an individual to part with biometric information much less through a network of private entities, even assuming that such a course is open to government, it cannot part with largess that would enrich private parties. The impugned action has caused extremely valuable biometric information to fall in private hands without regard to the stupendous monetary value of the information. Private entities have been allowed to obtain this information from citizens/ residents under the framework of the UID project without UIDAI or the Union Government having regard to the immense commercial worth of the biometric information that is being captured on privately owned computers and databases over which the government has no control or exclusive access. Indeed, the impugned project as worked in the field, extensively utilizes privately owned and operated infrastructure for capturing and storing biometric information. No control is exercised by either the UIDAI or any other government agency on the private entities and

their employees when these private entities cause the collection of biometric information. This information can be duplicated, replicated, transmitted and/or commercially exploited by individuals working for or in the private entities and / or by the entities themselves. The Union government and UIDAI have failed and neglected to perform their duty of ensuring that privately held biometric information is not susceptible to any type of misuse or exploitation by the parties collecting this information. They have also failed and neglected to discharge their primary duty of ensuring that huge commercial benefits that potentially could enure to the advantage of private parties because of their connection to the UID project and / or the AADHAAR scheme, are properly valued. Here, unique commercially valuable information is being garnered by private entities in the name of a governmental project with no assured machinery that will prevent the retention, exploitation or leakage of this information. The State has parted with largess and is facilitating the collection of biometric information by private hands, and is paying the private entities for this work without any tested technology or adequate legal framework in place that would guarantee the security or non-exploitation of the information. The impugned actions are palpably arbitrary and liable to be struck down.

Security of Collected Data

(I) In addition to the haphazard and unreliable manner employed by the 2nd Respondent in collecting data, it appears that there is no secure manner in which the 2nd Respondent will store data collected. The 2nd Respondent has failed to reveal to the public at large the manner in which the security of data is maintained and where and in what manner this data is going to be stored and secured. Different statements have been made by the 2nd Respondents from time to time, demonstrating the lack of clarity. It is submitted that there are no statutory safeguards with respect to the security of this data once it is collected. As set out herein, the process of collecting data is also extremely porous with no reliable protocols.

Surveillance

(J) There are several organizations within the government such as the Intelligence Bureau, Research and Analysis Wing (RAW); National Intelligence Grid, Multi Agency Centre and now the Central Monitoring System that operate outside legislative oversight. These organizations are exempt from the obligation of disclosure under the Right to Information Act and are not accountable directly to citizens/residents and constitutional authorities such as the Comptroller and Auditor General of India. Upon the UID number use becoming ubiquitous, the Petitioners apprehend that each of these agencies will be able to track individuals on a real time basis

increasing the scope of individual surveillance to a level that is impermissible under the Indian Constitution. Absent any statutory safeguard that prevents access to the information converged through the use of the AADHAAR number, the impugned project and scheme will result in impermissible levels of surveillance in violation of Article 14 and 21 of the Constitution of India. Copy of the list of organizations exempted from the purview of Right to Information Act is annexed hereto and marked as **ANNEXURE – P/2(COLLY) – (PAGES TO)**.

Invasion of Privacy

(K) The UID project as conceived and as being implemented will result in an extreme invasion of privacy and a violation of Article 21 in respect of persons who are issued a UID number. It is intended that the UID Number will become ubiquitous and will be required by a person at every stage of his or her daily routine. The manner in which the AADHAAR number is being propagated is that an individual will require to give this number when, for example, he or she operates a bank account or operates an ATM; visits a hospital or clinic for treatment; obtain delivery of a cooking gas cylinder; purchases goods; seeks to buy a ticket for travel by air or road or rail, etc. Moreover, the AADHAAR number may also be utilized together with a biometric information verification for entering into existing public building, private layouts, etc.

In this manner, at every step of a person's daily activity he or she will be subject to tagging, tracking and surveillance. The AADHAAR number is the key for enabling ease of surveillance when coupled with insistence by service provider to disclose the AADHAAR number for verification. At present, multiple forms of identifications are accepted by service providers and the consumer of services is not required to give the same identification at every place. The AADHAAR number with its biometric foundation (the reliability of which is known to be questionable), is liable to serve as the key tool for tracking and surveillance.

Private information of an individual is available in different 'silos' across service providers. For example, medical records of an individual may be available with one or more hospitals; the spending pattern records of a person may be available with the credit card company; the travel information regarding an individual may be available with the airline, etc. With the universalization of the AADHAAR number these information banks in unconnected silos will be easily bridged and all data on an individual will become very easily accessible to the State or persons who the State permits or persons who infiltrate the system, resulting in a destruction of privacy rights.

At the stage of collecting biometrics and other details, the handling of this information by unregulated private entity and their employees means that this information can be

accessed, duplicated, transmitted and traded in violation of a person's right to privacy. The impugned action is violative of Article 21 and potentially can severely undermine individual privacy as well as the larger issue on the right of a democratic community to be left alone without it being able to track individual movements of every person.

It appears that the Respondents are working in coordination with schools to enroll children as well as other persons connected with the schools. It is respectfully submitted that in addition to the points made above, this action is patently illegal inasmuch as children in schools do not have a legal capacity to consent and these children are being yoked to the Aadhaar apparatus for all time. It is respectfully submitted that no children ought to be compulsorily enrolled.

Undermining Human Dignity

(L) It is submitted that dignity is an important facet of the right to life under Article 21 of the Constitution. The right to live with dignity includes the right to be a member of society and engage in societal transactions and community affairs without unreasonable restrictions. The notion of dignity in an open society encompasses the right to services while remaining anonymous or at any rate without identifying himself or herself in a particular manner. Dignity implies that a person is entitled to the full range of services and citizens'

rights without having to part with biometric information. The impugned project assaults individual dignity by compelling persons on pain of exclusion from society, to part with biometric information. It impinges on dignity by universalizing the requirement of possessing and using an AADHAAR number.

Coercion To Part With Biometrics

(M) (i) Representations made by the UIDAI and the actions taken by it in propagating the UID scheme makes it clear that it wants to make the UID number a necessary pre-requisite for delivery of services and goods across the country. The UID number is not being issued only to disadvantaged persons who require some authentic identification before receiving benefits. The project is aimed at persuading public sector as well as private sector service providers to require residents to produce a UID number as an essential requirement for granting services. It is being represented that unless a person has a UID number, it will become extremely inconvenient for him/her to access essential services. In this manner, individuals are being and will be coerced into parting with their biometrics because otherwise essential services will be withheld from them. The element of coercion is present because there is no assurance from the Respondents that a citizen/resident or person will be extended all services without discrimination whether or

not she has or give her AADHAAR number. Such an assurance in law is essential to dispel the element of coercion. The impugned actions violate Articles 14 and 21 of the Constitution of India because they tantamount to denying essential services and rights except under threat of parting with biometrics.

(ii) It appears that the 2nd Respondent is actively canvassing with foreign embassies and missions to insist that applicants for visas must produce an AADHAAR identification. It is submitted that the right to travel abroad is recognized as a dimension of Article 21 of the Constitution of India and it is wrongful on the part of the 2nd Respondent to curb and fetter an individual right to travel overseas by requiring (through foreign missions) that an Indian who wants to travel abroad must have an AADHAAR number.

(iii) The Petitioners submit the action on part of the 2nd Respondent in seeking to actively promote the AADHAAR scheme through foreign mission and embassies is beyond the authority and remit of the 2nd Respondent and transgresses statutory limits delineated by the Passport Act, 1967. Copy of media report with respect to the 2nd Respondent promoting the use of AADHAAR number with embassies and missions is annexed hereto and marked as **ANNEXURE – P/3(COLLY) – (PAGES TO)**.

(iv) Illustrative of the coercion employed by different organs of the State are the following notifications/circulars/decisions taken by authorities that now insist upon the AADHAAR number or refuse services:

a) The Government of NCT of Delhi, Revenue Department has issued an order on 20-12-2012 making AADHAAR number compulsory for registration of marriages as well as for registration of documents in the Sub Registrar Offices.

b) Similarly, the State of Jharkhand has also made AADHAAR number compulsory for registration of marriages as well as for registration of documents in the Sub Registrar Offices.

c) The State of Karnataka has made AADHAAR number mandatory for availing benefits under government schemes such as social security pensions, LPG connection, ration card etc.

d) The Union Ministry of Petroleum has made AADHAAR number mandatory for 'Direct Benefit Transfer' scheme for LPG customers.

e) In the State of Maharashtra, AADHAAR number has been made mandatory for teaching and non-teaching employees in government aided schools for drawing salary.

f) The State of Kerala has made AADHAAR number mandatory for admission of students in schools and colleges.

g) The State of Himachal Pradesh has made AADHAAR number mandatory for admission of students in schools and colleges.

h) The State of Madhya Pradesh has made AADHAAR number mandatory for pension and provident fund.

i) The University Grant Commission has made AADHAAR number mandatory for students applying for scholarship or fellowship. AADHAAR number has been made mandatory by Employees' Provident Fund Organisation.

Copy of documents evidencing the above mentioned decisions where AADHAAR card has been made mandatory is annexed hereto and marked as **ANNEXURE – P/4(COLLY) – (PAGES TO)**.

(v) The 2nd Respondent has acknowledged that by the end of 2014 approximately 600 million individuals will stand enrolled under the AADHAAR scheme. Since the population of India is estimated in excess of 1.2 billion, it is obvious that more than half the population will not have AADHAAR number even at the end of 2014. In the circumstances insistence on the AADHAAR number as a prerequisite for extension of services is irrational and arbitrary inasmuch as it would mean that over half the population are denied services.

Failure to Provide an "opt out" Option

(N) The Petitioners submit that in order to pass the test of reasonableness and rationality, any scheme such as the AADHAAR scheme ought to have an option by which an individual may at any time opt out of the system. Quite apart from there being no informed consent when enrolling individuals, the failure to provide such an option violates Article 14 of the Constitution of India and also violates Article 21. Individual autonomy and dignity imply that if at some point a person would like to efface his or her data records then the person must be empowered to exercise such option. Otherwise, enrolment under the AADHAAR project is irreversible and amounts to parting with biometrics and demographic information as well as all other information that would be accessed from the use of the AADHAAR number. The Petitioners submit it is incumbent on the Respondents to extend to each and every person including every AADHAAR number holder an option to opt out of the AADHAAR scheme without adverse consequence and without any electronic trail or record being retained by the Respondents. It is submitted that "the right to be left alone" and "the right to be forgotten" are dimensions of Article 21 of the Constitution of India and these are transgressed by the failure on the part of the Respondents to provide an avenue to opt out and/or to delete all records collected through the use of the AADHAAR number.

Flawed Introducer System and Verifier System

(O) (i) The procedure adopted by the Respondent (through private entities) for securing enrolment for AADHAAR numbers includes a drive for enlisting individuals. The process of enrolment for those persons who do not have identification documents and who require to be introduced to the system, involves an agent called the "introducer" who vouches for the enrollee. The 2nd Respondent has laid out criteria for who can act as an introducer. These criteria do not require the "introducer" to know the person he is introducing, thereby compromising the integrity of the entire enrolment process. The Union Home Ministry has expressed serious concern about this loose and unreliable methodology being worked for enrolment. Copy of a media report referring to the position taken by the Union Home Ministry on the process of using "introducers" is annexed hereto and marked as **ANNEXURE – P/5(COLLY) – (PAGES TO)**.

(ii) Similar to the flawed introducer system, the verifier system adopted by the 2nd Respondent also suffers from severe limitations that compromise the integrity of the project. Where a person does not have reliable documents to identify himself or herself, the Respondent permit enrolment on the basis of an identification document issued by "verifiers" who are recognized by the 2nd Respondent. These

verifiers issue certificates /identification documents without being subject to any level of oversight and there have been instances of abuse of this process in the State of Andhra Pradesh. Copy of a media report on misuse/abuse of the verifier system is annexed hereto and marked as **ANNEXURE – P/6(COLLY) – (PAGES TO)**.

Dismantling of Public Distribution

(P) Although styled as a programme that is designed to help the disadvantaged, in fact the impugned project is likely to cause great harm to this section. A large number of essential items such as food, kerosene, etc. are distributed by the government to disadvantaged segments of society through a public distribution system. The public distribution system has a vast network of shops, outlets, warehouses, etc. as well as a supporting distribution network. The UID number coupled with cash transfers to individuals is bound to result in the dismantling of the entire PDS infrastructure and network. Having regard to the untested biometric technology being employed, the simultaneous dismantling of the PDS infrastructure without validation of the efficacy of the AADHAAR project, is arbitrary and violative of Articles 14 and 21 of the Constitution of India.

Unreliability of Biometrics

(Q) (i) The biometrics being collected are an extremely unreliable basis for identifying an individual on a national

scale for a country as populous as India. It is an unproven technology which has been abandoned elsewhere in the world. Where individuals are engaged in manual labour which applies extensively in the Indian context, the ridges on a finger are apt to wear out. This is an extremely common condition amongst construction workers, farm labourer, etc. Likewise, older person's finger prints are difficult to capture at the time of creating the biometrics database and also at the time of validation. Biometric information may be affected by the aging process, disease, stress and occupational factors.

(ii) In so far as the Petitioners are aware, the state of knowledge with respect to the reliability of biometric information of persons residing in India was very poor at the launch of the impugned programme. Indeed, on or about February 2010 the 2nd Respondent issued a notice inviting applications for a consultant who could advise the authority on issues relating to biometrics. This notice itself acknowledges the total absence of information relating to biometrics. Copy of 2nd Respondent's notice inviting applications on or about February 2010 is annexed hereto and marked as **ANNEXURE – P/7-(PAGES TO)– (PAGES TO)**.

(iii) It appears that the 2nd Respondent has commissioned studies to evaluate the reliability of biometrics for enrolment

and authentication on or about September 2009 by constituting 'UIDAI Committee on Biometrics'. This 9 member committee included the Registrar General of India, the Joint Secretary from Ministry of Rural Development, a Member from the Reserve Bank of India, representatives from Indian Institute of Technology etc. The Petitioners verily believe that these studies confirm the flaws in the use of biometrics for these purposes. The following are some critical observations of the committee:

> "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."
>
> "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."

The Petitioners state that there are other independent studies conducted across the world which also reflect upon the unreliability of biometric data. A copy of one such independent study 'Template Aging in Iris Biometrics: Evidence of Increased False Reject Rate in ICE 2006' by Sarah E. Baker, Kevin W. Bowyer, Patrick J. Flynn and P. Jonathon Phillips is annexed hereto and marked as **ANNEXURE – P/8 – (PAGES TO)**. The Petitioners will rely on copies of further studies, when produced.

(iv) The biometric system being employed has not been effectively tested in India on an appropriately representative scale such that it would justify the enormous expenditure being undertaken on the impugned project. Tax payers' money and government funds are being poured into a technology that has failed elsewhere and which had not been adequately validated in the Indian context. The impugned project suffers from the vice of arbitrariness.

Biometrics Exceptions

(R) Apart from the unreliability of biometrics generally, for certain segments of the population biometrics in the form of finger print and iris scans are not possible to capture because of physical limitations. For instance, persons engaged in hard manual labour or elderly individuals may

find that the ridges on their fingers are not distinct enough to capture for de-duplication and authentication. Likewise, the iris scan of a person suffering from cataract may not yield a reliable result. Individuals whose biometrics cannot be captured are treated as biometrics exceptions by the Respondent. No reliable alternative method is adopted by the Respondents when issuing AADHAAR numbers to such persons and this has not only compromised the data base but is facilitating fraud. Illustrative of the misuse in this regard is a Hyderabad case with regard to which the relevant documents, a copy whereof is annexed hereto and marked as **ANNEXURE – P/9 – (PAGES TO).**

FACTS LEADING TO THE FILING OF THIS PETITION

9. The UIDAI is a department of the Union Government functioning within the Planning Commission. UIDAI was notified by the Planning Commission on 28.1.2009. Subsequently, on 2.7.2009, the Government appointed Shri Nandan M. Nilekani as Chairman of the UIDAI. Copy of the notification dated 28.01.2009 is annexed hereto and marked as **ANNEXURE-P/10-(PAGES TO)**.

10. Although the programme was launched in September, 2010, the 1st Respondent introduced the National Identification Authority of India Bill, 2010 in Parliament on 3.12.2010. This Bill was referred to the Parliamentary Standing Committee on Finance which tabled its report in Parliament in 13.12.2011. The Committee found that the

Bill was wanting in several respects. The report of the Committee states:

> "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."

A copy of the report submitted to Parliament by the Parliamentary Standing Committee on Finance is annexed hereto and annexed marked as **ANNEXURE – P/11 – (PAGES TO)**.

11. The Respondents have not introduced any fresh legislation since then and the project has continued without any legislative framework.

12. The UIDAI's mission is to issue a Unique Identification Number (UID) that can be verified and authenticated online.

13. AADHAAR is the UIDAI brand and logo. Consequently, the UID number is also commonly referred to as the AADHAAR number.

14. The AADHAAR number is a random 12 digit number which is unique for all residents in India. The programme was launched in September, 2010 in rural Maharashtra and had now been extended across India.

15. AADHAAR is intended to be a single source of verification of identity and will link a person's passport number, driving licence, PAN card, voter ID card, bank account address, etc. Although the scheme is touted as being voluntary, as more particularly set out herein, the intent of government is to make it mandatory by

aggressively promoting the use of this number amongst service providers. The object is that these service providers will over time insist upon production of the AADHAAR number making it extremely inconvenient to a person not holding a UID number to live and function freely and efficiently in society. Government and the UIDAI are actively requiring personal biometrics to be yielded to databanks in this manner.

16. There is no certainty about the cost of the project. The estimates have risen sharply and it is now expected to cost in excess of Rs.1,50,000 crores.

17. The UIDAI is implementing its project through numerous networks, the most significant of which for the purposes of this petition are the following:

A. Collection network through Registrars and Enrolment Agencies;

B. Technology creation network to implement biometrics identification systems and the storage of information obtained; and

C. Network with government and private agencies to spread the utilization of AADHAAR numbers.

The material facts in respect of each of these structures is described below.

<u>System for Collection of Biometric Information</u>

18. UIDAI does not directly collect any biometric information. It has entered into arrangements with "Registrars". There is no statutory

or administrative definition of who qualifies to act as a Registrar. The UIDAI has entered into MOUs with State Governments which require the government to identify departments within government to act as Registrars. This may include departments such as the Consumer Affairs Department or the Civil Supplies Department.

19. The Registrars are allowed to collect such information as they consider necessary even beyond the information required by the UIDAI, depending upon the needs and requirements of the Registrars. However, Registrars themselves do not have the capacity to enroll persons and collect the information.

20. The Registrars, in turn, engage private sector "Enrolment Agencies" who are empanelled with the UIDAI. These enrolment agencies have designated territories where they may conduct their enrolment work. It appears that out of 220 enrolment agencies, 11 were dis-empanelled by the UIDAI in January 2011.

21. Although collected under the banner of the AADHAR project and actively projected as a government exercise no government agency takes responsibility for "cradle to grave" security and safety of the biometric information collected. Specifically, UIDAI takes no responsibility for the security of the personal biometric data being collected. The data is initially collected and stored on computers that do not belong to the UIDAI or the Registrars. The information collected becomes the property of the private individual / private enrolment agencies and can be used by these private parties as they like. There are no effective and enforceable security protocols that ensures that the private enrolment agencies do not misuse the

information in their hands. There is no effective and enforceable machinery by which a private enrolment agency can be restrained from duplicating, transmitting or retaining the information obtained through the enrolment process. UIDAI and the Union Government have both failed and neglected to create a system with technological and legal integrity that would protect the biometric data of millions of Indian citizens and residents which is being collected on private computers. This is a case of ineptitude, negligence and violation of public trust. The state is causing residents and citizens to part with vital personal information without any security framework regarding the protection of this data and this data or any machinery to retrieve data that has fallen into the wrong hands.

22. Information collected by the enrolment agencies and the data captured is transferred to UIDAI's Central ID Repository (CIDR) via memory sticks through courier services or by directly uploading the data to the CIDR. Each of these methods is fraught with potential leakages and there is absolutely no safety in respect of the data being collected.

23. The empanelled enrolment agencies comprise private sector companies, trusts, proprietary concerns / firms, foundations, public limited companies and a range of other entities. The UIDAI does not appear to have empanelled these enrolment agencies on the basis of an established track record of impeccable integrity in preserving and protecting sensitive data. There is no guarantee or assurances regarding what has happened to data already collected

and what may happen to data lying with these parties or which may be collected in the future. There is absolutely no screening with regard to the employees of these organizations or their background. There is also no manner in which the UIDAI or the Registrars can check on whether employees of the Registrars and/or the enrolment agencies are misusing the sensitive biometric data which comes under their control. There also does not appear to be any provision either in law or in the contracts entered into by the UIDAI and the enrolment agencies / Registrars with regard to the ownership of the data.

A copy of the MOU entered into between the UIDAI and the Government of NCT, Delhi is annexed hereto and marked as **ANNEXURE – P/12 – (PAGES TO)**. A copy of the list of 209 enrolment agencies is annexed hereto and marked as **ANNEXURE – P/13 – (PAGES TO)**. A copy of the list of 11 enrolment agencies dis-empanelled in January, 2011 is annexed hereto and marked as **ANNEXURE – P/14 – (PAGES TO)**.

System for Creating Technology to Process and Store Information

24. It appears that the UIDAI has entered into arrangements with four consortia to implement the core biometric identification system in support of the AADHAAR Project. These three consortia are entrusted with the task of designing, supplying, commissioning, maintaining and supporting the Biometric Identification System. They are involved in the development of software for enrolment

stations, verification of the data and other tasks for validation. The leaders of the three consortia are (i) Accenture; (ii) Mahindra Satyam & Morpho joint venture; and (iii) L1-Identity Solutions.

25. L1 Identity Solutions is a large American defence contractor based in Connecticut. It specializes in biometric technology systems and several of its officers and Directors have served with the Central Intelligence Agency (CIA) and other American defence organizations. The former Director of the CIA, Mr. George Tenet, is on the Board of Directors of L1 Identity Solutions. L1 Identity Solutions has contracts with the US Department of Defence and other intelligence agencies. This information is relevant because biometric impression of Indian citizens and residents can be easily transmitted to foreign governments who will then have access to the biometrics of Indian residents, potentially imperiling national security and severely undermining the privacy and autonomy of individuals.

Partnership with State Governments and Service Providers

26. It appears that the 2nd Respondent has introduced a new data sharing policy with State Governments for sharing of data collected by it on a request made by the State Government. This 'Data Sharing Policy' records that State Governments expressed reservations about not having access to the information collected under UID Project and to resolve the issue, the 2nd Respondent has agreed to make data available to the State Government for welfare and public services. Although this policy purports to have certain

checks and balances, firstly, it strengthens the apprehension raised by the Petitioners in this petition that the sensitive personal information being collected is capable of being transmitted easily on a request of a party. Secondly, 2nd Respondent is not accountable for such harm as it is not under any legislative control in case of misuse of information. Thirdly, this policy also fails to ensure that the recipient of information does not part with or duplicate the information for its own retention. It is submitted that these ramifications are not explained to persons giving the information under the UID Project and amount to grave violation of right to life and personal liberty. Copy of the Data Sharing Policy introduced by the Respondents is annexed hereto and marked as **ANNEXURE – P/15 – (PAGES TO)**.

GROUNDS

27. In paragraph 7 of this petition, detailed grounds are set out explaining why the impugned UID project and AADHAAR scheme are ultra vires, illegal null and void. For the sake of brevity, the Petitioners are not repeating the grounds. Each of these grounds is pressed in the alternative and without prejudice to one another.

JURISDICTION

This petition is preferred to this Hon'ble Court under Article 32 of the Constitution of India having regard to the violation of Articles 21 and 14 of the Constitution of India as explained above. Having regard to the nation wide implications of important issues raised in

this petition, this Hon'ble Court ought to entertain and hear the present petition. The Petitioners state that they have not filed any other similar petition before this Hon'ble Court or any High Court.

This petition assails the UID Project and AADHAAR scheme on diverse grounds. The frame of the challenge in this case is wider than those urged in Writ Petition (C) No. 494 of 2012 (Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.) wherein notice was issued by this Hon'ble Court on 30.11.2012.

PRAYER

In the above facts and circumstances of the case, it is most respectfully prayed that this Hon'ble Court may be pleased to:

a) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India declaring the UID project and AADHAAR scheme as being ultra vires Articles 14 and 21 of the Constitution of India, illegal, null and void;

b) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, ordering and directing the Respondents by themselves or through their officers and agents to forthwith forbear from taking any steps in implementation or in furtherance of the UID project or the AADHAAR scheme;

c) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, ordering and directing the

Respondents by themselves or through their officers and agents to forthwith cease and desist from taking any further steps to enroll individuals and/or collect biometric information and/or issue AADHAAR numbers to them;

d) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, ordering and directing the Respondents by themselves or through their officers and agents to forthwith destroy all data and information collected from individuals;

e) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, ordering and directing the Respondents by themselves or through their officers and agents to to ensure that each and every service provider using the AADHAAR number for identification also extends the service to all persons with alternative identification, on a non-discriminatory basis;

f) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, ordering and directing the Respondents by themselves or through their officers and agents to to obtain all data (biometric and other) that was taken from individuals under the AADHAAR scheme/ UID project and which now lies with private parties and to destroy all such data within a time bound manner;

g) Issue an appropriate writ, order or direction under Article 32 of the Constitution of India, restraining all private parties and government organizations in custody or control of any data (biometric or other) that was taken from individuals under the AADHAAR scheme/ UID project and which now lies with private parties, from in any manner retaining or using this data.

h) Issue an appropriate writ, order or direction declaring that no service or supply of goods of any type offered by government or private party may be withheld from a person on the basis that he or she does not have an AADHAAR number;

i) award costs relating to the present petition to the Petitioners; and

j) Issue any other writ/order/direction in the nature of mandamus as this Hon'ble Court may deem fit and proper in the circumstances of the case.

AND FOR THIS ACT OF KINDNESS, THE PETITIONERS SHALL, AS IN DUTY BOUND, EVER PRAY.

FILED BY:

M/s. K.J. JOHN & CO.,
Advocates for the Petitioners

DRAWN ON: 02.09.2013

FILED ON: 03.09.2013

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION
CIVIL WRIT PETITION NO. OF 2013

IN THE MATTER OF:

Mr. S.G. Vombatkere & Anr. ...Petitioners

Versus

Union of India & Ors. ...Respondents

AFFIDAVIT

I, Bezwada Wilson, S/o Late Shri Yacob, aged about 47 years, R/o 36/13 Ground Floor, East Patel Nagar, New Delhi, do hereby solemnly affirm and state as follows:-

1. I am the Petitioner No. 2 herein, I am fully conversant with the facts and circumstances of the present case and am as such competent to swear the present affidavit on behalf of the Petitioners.

2. I have gone through the contents of the accompanying List of Dates and the Writ Petition running into pages " " to " " and have understood the list of dates at pages " " to " " and paras " " to " " of the Writ Petition and say that the facts set out therein are true to my knowledge as derived from the records maintained by the Petitioner and the submissions made therein are on legal advice received from the Advocates and believed to be true and correct.

3. I say that the Annexures P/1 to P/ to the accompanying Writ Petition are true and correct copies of their respective originals.

4. I say that no facts which were not pleaded before the Court below have been pleaded in this Court.

DEPONENT

VERIFICATION:

Verified at New Delhi on this 17th day of August, 2013, that the contents of paragraphs 1 to 4 of my above affidavit are true and correct that no part of it is false and nothing material has been concealed there from.

DEPONENT

ANNEXURE-P/1 (COLLY)

Petitioner No.1 i.e. Sudhir Vombatkere's profile.

The 1st Petitioner is a citizen of India and is aged about 71 years. The 1st Petitioner is a retired Indian Army officer who retired after 35 years in uniform in the rank of major general from the post of Additional DG in charge of Discipline and Vigilance at Army HQ, New Delhi. He has been awarded the Visishta Seva Medal (VSM) by President of India in 1993 for his distinguished service rendered in Ladakh.

He holds a PhD degree in civil structural dynamics from I.I.T., Madras. After retirement, he is engaged in voluntary social work at Mysore and other areas around Karnataka. The 1st Petitioner is also an Adjunct Associate Professor in International Studies of the University of Iowa, USA and teaches under graduate students from USA and Canada in programs where the students visit Mysore.

In so far as the Unique Identification Project ("UID project") is concerned, the 1st Petitioner has written various articles pointing out the security risks of the project.

THE HINDU

Published February 6, 2013 00:30

The architects of the unique identification scheme are yet to provide satisfactory answers to concerns about data security.

The Aadhaar scheme of the Unique Identification Authority of India (UIDAI) is to provide India's billion-plus people with a unique identification number. Enrolment is not mandatory, though it was mentioned that it would be difficult for people to access public services if not done. The scheme requires individuals to provide their photograph, fingerprints and iris scan along with documentary personal information for data capture by outsourced operators. It is meant to bypass the corrupt bureaucratic system and deliver government subsidies and grants to the poor, and bring them into the banking system. Sceptics argue that it is an effort to capture the funds of hundreds of millions of micro- and nano-investors who are today outside the banking system, to bring them into the credit economy.

The scheme was introduced as a pilot project in Karnataka's Mysore district. The poor and those who survive on daily wages were not enthusiastic about

enrolment, because it meant losing four or five days wages, to stand in queues, to fill up forms, to produce documents, to provide biometrics, etc., and, later, to open bank accounts. The UIDAI overcame the initial reluctance by wide advertisement of the benefits of enrolment. When this too did not achieve the target set, the local administration informed the public that PDS ration and LPG supply would not be available without the Aadhaar number. This resulted in serpentine queues right through the day at enrolment centres, at the end of which the UIDAI could claim that 95 per cent of Mysoré district's population had enrolled itself into the scheme.

Media reports indicate that commencing January 1, 2013, MGNREGA, the Rajiv Gandhi Awas Yojana (RGAY), the Ashraya housing scheme, Bhagyalakshmi and the social security and pension scheme will be linked with Aadhaar in Mysore district. This linking, with rights like salary and pension, and important entitled benefits and services, has raised some hackles because enrolment is not mandatory.

It has led to questions on whether salary and pension rights, and benefits like PDS ration and LPG supply can be denied just because an individual does not possess a unique Aadhaar number. Today, teachers in Maharashtra and government employees in Jharkhand cannot draw

their salaries. Apart from pro-poor projects like MGNREGA and RGAY, even jobs, housing, provident funds and registering a marriage now require enrolment. From being not mandatory, the "poor-inclusive" Aadhaar scheme appears to have quietly metamorphosed into becoming exclusionary and non-optional.

The UIDAI's own Biometrics Standards Committee stated that retaining biometric efficiency for a database of more than one billion people "has not been adequately analysed" and the problem of fingerprint quality in India "has not been studied in depth." Thus the technological basis of the project remains doubtful.

Criticism from the top

However, the severest critic of the entire scheme has been the Parliamentary Standing Committee on Finance (PSCF), which deliberated that the Aadhaar scheme is "full of uncertainty in technology as the complex scheme is built upon untested, unreliable technology and several assumptions." It found Aadhaar to be "directionless" and "conceptualized with no clarity." But the UIDAI shelters under the Prime Minister's protective wing and continues to stonewall not only public queries and criticism, but also the unequivocal verdict of the PSCF.

Possibly even more serious is data security, and the consequent threat to privacy. The UIDAI claims that access to its database will be secure from intelligence agencies. This claim is hollow, because the Aadhaar project is contracted to receive technical support from L-1 Identity Solutions (now MorphoTrust USA), a well-known defence contractor. Contracts are also awarded to Accenture Services Pvt. Ltd., which works with the U.S. Homeland Security, and Ernst & Young to install the UIDAI's Central ID Data Repository. It is impossible to ensure database security when technical providers are American business corporations, and U.S. law requires them to provide information demanded of them, to U.S. Homeland Security. But the UIDAI is in denial.

If biometric data and other personal information fall into the hands of unauthorised agencies, privacy is unequivocally compromised. Compromising an individual's personal data affects only that person, but when the personal data of many millions of people is involved, there is potential for a national disaster. The fact that the UIDAI is silent on or evasive about these security concerns does not inspire confidence in the capability of the UIDAI or the Aadhaar system to maintain the right to personal privacy.

Though the Aadhaar project is "not mandatory," enrolment by threat of exclusion from availing benefits and services, and threat of denial of rights like salary or pension makes it non-optional. This kind of deviousness is unbecoming of a democratically elected government. Coming on top of many huge scams, the present government may suffer electorally if it persists in using unethical, extra-legal coercion to impose the security-defective, technologically unproven, very expensive UID Aadhaar scheme on the public.

(Major General S.G. Vombatkere, who retired as Additional Director General, Discipline & Vigilance in Army HQ, New Delhi, writes on strategic and development-related issues.)

Keywords : Aadhaar scheme, Unique Identification Authority of India, Biometrics Standards Committee, MGNREGA, PDS ration, Rajiv Gandhi Awas Yojana

ANNEXURE-P/2 (COLLY)

CIC ONLINE

Exempted organizations

The List of 22 exempted organizations is given

RTI Manuals

The list of 22 exempted organizations is given below:

RTI Act

Intelligence Bureau, Ministry of Home Affairs

Guide For the Public Authority

Directorate of Revenue Intelligence, Ministry of Finance

Guide Fr First Appellate Authority

Central Economic Intelligence Bureau, Ministry of Finance

Guide For The Central Public Information Officers

Directorate of enforcement, Ministry of Finance

Guide For the Information Seekers Under the Right to Information Act, 2005

Narcotics Control Bureau

Exempted Organizations

Aviation Research Centre

Special Frontier Force

Border Security Force, Ministry of Home Affairs

Central Reserve Police Force, Ministry of Home Affairs

Indo-Tibetan Border Police, Ministry of Home Affairs

Central Industrial Security Force, Ministry of Home affairs

National Security Guard, Minister of Home Affairs

Research & Analysis Wing of The

Cabinet Secretariat

Assam Rifles, Ministry of Home Affairs

Sashastra Seem Bal, Ministry of Home Affairs

Special Protection Group

Defence Research and Development Organization, Ministry of Defence

Border Road Development Organization

Financial Intelligence Unit, India

Directorate General Income Tax (Investigation)

National Technical Research Organization

National Security Council Secretariat

Govt keeps Natgrid, NIA out of RTI ambit

AMAN SHARM New Delhi, June 21, 2011/ 10:11

The National Intelligence Grid is Home Minister P. Chidambaram's pet project.

Here's another blow to transparency in the government. After exempting the CBI, the government has now pushed the National Intelligence Grid (Natgrid) and the National Investigation Agency (NIA) out of the ambit of the Right of information (RTI) Act.

Putting Natgrid in the list of organizations exempted from making disclosures under the RTI Act will certainly fuel concerns as a citizen would not be able to seek details on whether any of his databases have been accessed by the investigating agencies through Natgrid.

With the inclusion of Natgrid, NIA and CBI in the second schedule to the RTI Act- a decision which was made official through a gazette notification on June 9- there are now 25 intelligence and security' organizations which are exempted from providing any information under RTI Act. Except information pertaining to allegations on any corruption and human right violations.

To start off in 2005, the second schedule had 18 organizations on its list, which grew to 22 in 2008 and to 25 presently.

Most of the 11 agencies which can access Natgrid for getting database information on a citizen are also already exempted from the RTI Act.

A government source said Natgrid needed to be kept out of the RTI purview because most of the 11 agencies authorized to access databases through the Natgrid are already exempted from RTI. "So anyway if a citizen wants to know if the Intelligence Bureau (IB) asked for any

information on his bank account database through the Natgrid, the information cannot be disclosed as IB is an exempt organization, Natgrid is not an organization but only a forwarding tool and like an extended server of these 11 agencies, "the source said.

Supreme Court lawyer and cyber law expert, Pawan Duggal, however, said the decision to exempt Natgrid from the RTI Act only strengthened the 'Big Brother' concept. "It is huge setback to transparency. It's like a blackout. We agree that national sovereignty is paramount but that is not tantamount to removing all levels of transparency," he said

Aadhaar may help in visa processing too: UIDAI chairman

TNN Jun 30, 2013

BANGLAORE :Foreign embassies could probably are Aadhaar, the 12-digit unique identification number, as a tool to simplify visa processes in the future, according to UIDAI chairman Nandna Nilekani.

"We're having preliminary discussions with some embassies who said they can use Aadhaar to simplify visa process. Embassies spend a lot of time verifying a person's identity.

If Aadhar helps to streamline that, it could be good for them. It's really up to the imagination of people when the platform is opened up to developers," he said on the sidelines of The 2013 Conference of Working Group 8.6 of the International Federation for Information Processing (IFIP) here on Saturday.

The government has launched an application programming interface (API) to develop applications using the Aadhar platform. Like Google and Apple which have opened up their platforms to developers to write software applications, Nilekani believe in thriving app ecosystem will emerge around the Aadhaar platform that would enhance service delivery and user experience.

"We believe unique ID verification is fundamental to a whole host of service delivery. An open architecture of APIs allows different people to build applications around the unique ID system. Apps and enrollments will create a virtual cycle which will create the momentum for us to get everyone on board", he added.

The Aadhaar platform will create a bouquet of applications around Know Your Customer (KYC), transactional services and maintaining other personalized digital assets like credit history and health records on the cloud for which

identification is a prerequisite. "The RBI has said banks can use Aadhaar for authentication and KYC purposes. More people are saying it's a KYC to get access to a particular public service. As they start using the electronic KYC, they'll get instant access to services at any point," he added.

Enrollment cost

Nandan Nilekani said the Aadhaar project cost is estimated at $3-$4 billion with each enrollment costing Rs.100-150. He said the UIDAI has built a robust process to authenticate biometric details of enrolled people. "Currently, we have enrolled 440 million people and we enroll 8 lakh-10 lakh people every day. We do biometric deduplicaiton with 99.99% accuracy, we might have 0.1% error and therefore, we'll use other techniques to scrub data," he added.

Virtual Ellis Island

Aadhaar is a digital ID. It's a number on the cloud associated uniquely with a person. You can think of this as a virtual Ellis Island (gateway for millions of migrants to the US) where people outside the system are entering the system for the first time and getting an identity).

ANNEXURE - P/3

Aadhaar's next mission: Simplify visas?

DC | 30th Jun 2013

Bengaluru: Nandan Nilekani's big idea, the Aadhaar number, is gaining both adherents and "allies" as the numbers of people with a unique identity grow rapidly – some 800,000 to a million people are enrolling for the UID daily.

After various departments of the Indian government have hitched on the Aadhaar for 'know your customer' requirements and, increasingly, transactions, foreign embassies are now exploring the possibility of using the Aadhaar number to simplify their visa processes.

Nilekani, who mentioned the development during a during a talk at IIM-B on Saturday, said that the UID Authority had had "preliminary discussions" with some embassies, but hastened to add that the Aadhaar only authenticates identity but is not proof of citizenship.

"They (consulates) can look up the Aadhaar number, since they require verification of one's identity. However, it is only an idea at this stage, and I can't comment much about it."

56

ANNEXURE-P/4(COLLY)

GOVERNMENT OF NCT OF DELHI
REVENUE DEPARTMENT
5, SHAM NATH MARG DLEHI-110054

No.F.10(6)/CCS/DivCom/Hqrs/5130-5131

Dated: 20.12.2012

ORDER

It has been decided to use the Aadhaar platform for the delivery of various services rendered by the Revenue Department. Hence, it is considered necessary that the Aadhaar information of the applicants seeking the various services from the Revenue Department is to be compulsorily given at the time of applying for the service.

It is henceforth ordered that AADHAAR No. of the applicant, will be required to be mentioned compulsory at the time of applying various services as mentioned below. The Aadhaar Card information of the applicants should be mentioned in the prescribed Applicants Forms.

1. Registration of Marriages under Hindu Marriage Act.
2. Registration of Marriages under Special Marriage Act.

3. Solemnization of marriages.

4. Registration of various documents in the Sub Registrar Offices.

Specimen of the modified application forms of the above services are available on the website of Revenue Department (http://revenue.delhi.gov.in). The guidelines on "How to Integrate the Aadhaar for the various services rendered by Revenue Department, GNCTD" are also available at this link and are enclosed with this order.

All the Deputy Commissioners are directed to ensure that this order is prominently displayed in the Notice Boards of the respective districts. General public may also be informed through permanent display of these conditions in the Notice boards of the Revenue Department/District and also in the offices of Sub Registrar Offices. This order will come into effect from January 1, 2013.

This issues with the prior approval of the Secretary (Revenue).

Sd/-
(Rajiv Kumar)
SDM (HQ)

No.F.10(6)/CCS/DivCom/Hqrs/

Copy to:-

1. All Deputy Commissioners,
2. All ADMs, Delhi
3. All SDMs, Delhi
4. All Tehsildars, Delhi
5. All Sub Registrars, Delhi
6. All SDMs (Hqrs)
7. SIO, Delhi State NIC HQ, Delhi Sectt, IP Estate Delhi.
8. System Analyst to upload the order on the department's website.
9. OSD to the Chief Secretary
10. PS to Secretary (Revenue)
11. PA to Special Secretary (Revenue)

Sd/-
(Rajiv Kumar)
SDM (HQ)

My Aadhaar Card A Complete Guide to Aadhaar and Aadhaar Enrollment

Aadhaar mandatory for marriage and property registration in Jharkhand

In a bid similar to Delhi government, the state government of Jharkhand has also decided to make Aadhar card mandatory for marriage registry purpose. Besides marriage registration, the state government has also made Aadhar card mandatory for property registration as well. The registry department has also been directed by the government about these changes in the present system. Under this new scheme not only the buyer and seller of the property but also the witnesses have to produce their, Aadhaar details in order to complete the registration process. Since still a large section of people in the state have not got their Aadaar numbers, this implementation will be effective from January 1 next year at any cost. If one has got Aadhar card but is denying of having it then it will be considered an offence by him and provision of FIR is also applicable under such condition.

Besides marriage and property registration, Aadhaar card will also be mandatory for those students who wish to take advantages of pre-matric and post-matric scholarship programs in Jharkhand. This decision was

taken during a review meeting of E-Kalyan Yojana last week. The bank accounts of the students will be linked with their Aadharr numbers and the funds of the scheme will be transferred directly into the student's bank account making the whole process transparent and fast.

The continuous oppose to Aadhaar from the students of JNU has finally started to weaken as a new circular was issued in the campus asking students to enroll for Aadhaar in order to get scholarship benefits. The circular was anticipated much earlier because of the move of UGC to link Aadhaar with the scholarship programs. Student's Union at the JNU is still not in favour of such type of implementation attributing to useless fatigue to the students. The students at the campus have not been in with the idea of Aadhaar since the very beginning but now they are compelled to enroll for UID number in order to obtain their scholarship amounts

1. Get your Aadhar before registering your marriage
2. Now Aadhar valid for applying for passport
3. Adhaar mandatory for scholarship and fellowship
4. Aadhar card mandatory for new EPFO members

DECCAN

HERALD

Wednesday 03 July 2013

State makes UID must for govt scheme entitlements

Nandini Chandrashekar, Bangalore, June 9, DHNS:

Not revealing info can lead to temporary suspension of services

Privacy concerns abound about each citizen of this country being issued an identity number, but the State government is firmly going ahead with its plans to include every citizen in the Unique Identification plan.

Recently, the State government issued an order making it mandatory for people availing of benefits from seven government schemes offered by six departments to furnish all information, while enrolling for UID or Aadhaar project. If information is not revealed, the services could be suspended temporarily.

The Karnataka Resident Data Hub project envisages integrating UID numbers to the various subsidy-linked services offered by the government. Linking this would help them prevent pilferage and leakage of services and also eliminate duplicate and ghost entries. Towards this purpose, the government has decided to make seven major services 'Aadhaar enabled.' These are

social security pensions, IP pumpsets, membership of Milk Co-operative Federations, Bhagyalakshmi scheme, LPG connection, ration card and Mahatma Gandhi National Rural Employment Scheme (MGNREGS).

'Mandatory'

Conversely, it means that anyone who need to be a beneficiary or would like to continue availing of these services, will need to get an UID.

"It is implied in the order", declared an senior official confirming the worst fears of many anti-UID advocates that it will be made mandatory.

The government is also offering a carrot by paying an incentive of Rs.100 per head to BPL category entitlements under social security schemes and MGNREGS , if they offer relevant documents.

According to the latest statistics, 4.5 million people have enrolled in Tumkur and Mysore and enrolment in other parts of the state will begin on June 27 in Gulbarga and Dharwad.

The enrolment for the entire State is expected to be completed by 31 March, 2012.

Joy Mukul, New Delhi May 15, 2013

Aadhar compliance made mandatory for LPG subsidy

Domestic LPG consumers in 20 districts would now have to get the aadhar number and seed it with their bank accounts to avail of subsidy on nine cylinders. This exercise would have to be completed in three months starting June 1 after which they would lose their entitlement for subsidy.

The mandatory requirement of aadhar number and its seeding is part of the Direct Benefit Transfer (DBT) scheme for LPG customers announced today. Addressing a press conference, Petroleum minister Mr Veerappa Moily said, "Reciprocal initiative has to be taken by consumers."

He said all LPG consumers would get an advance in their bank account as soon as they book the first subsidize cylinder even before delivery. This is to reduce their financial burden when they purchase the first LPG cylinder at market rate after launch of the scheme." As soon as, the first cylinder is delivered to such consumers, subsidy eligible on date of delivery will again get credited in the bank account, which will then be

available for the purchase of the next cylinder at the market rate.

The launch of DBT in LPG is the biggest programme under the government policy of direct credit of subsidy. There are 14 crore LPG consumers in the country which comprises 60% of the population. "So, the first step is a small one," said Vivek Rae, secretary, ministry of petroleum and natural gas.

On the question of why Aadhar has become compulsory, Rae said it was needed to credit LPG subsidy into bank accounts.

"If you want LPG subsidy then aadhar is compulsory." After the grace period of three months, as soon as a consumer links the Aadhar number to bank account and in LPG database, one-time advance and subsidy transfer will re-commence as per the balance entitlement.

There is 89% Aadhar penetration in these districts with 52% seeding with LPG data base of some 75 lakh consumers in the 20 districts. Seeding with bank account is 15%. The 20 districts include five in Andhra Pradesh, four in Himachal Pradesh, two each in Karnataka, Kerala and Madhya Pradesh, one each in Dam and Diu, Goa, Maharashtra, Pondicheery and Punjab.

An assessment would be done after a month. "We will review the scheme and then extend to other districts, he said. Once implemented, the government will transfer close to Rs 4,000 to every household annually to enable people to buy nine cylinders of LPG at the current market price.

Currently, state-owned oil firms sell domestic cooking gas at a highly subsidized rate of Rs 410.50 per 14.2-kg cylinder. Consumers are entitled to get nine cylinder of 14.2-kg each at the subsidized rate in a year. Each consumer will get a little less than Rs 4,000 annually but will have to buy LPG at market price. One fourth of LPG subsidy would be released by the ministry of finance every quarter to oil marketing companies who will be responsible for crediting it into the account of LPG consumers.

What consumers need to know?

* Get an Aadhaar number if they don't have one at Aadhaar enrollment centers.

*Open a bank account with Aadhaar number if they do not have one by going to a bank branch with Aadhaar number

OR

*If they already a bank account then link their Aadhaar number with their bank account by visiting their branch or through a request form available with LPG distributors and deposit it in the drop boxes placed at LPG distributors premises.

*Provide Aadhaar numbers to LPG distributors for linking with LPG consumer number.

67

Aadhar card compulsory for Maharashtra govt school staff for drawing salaries

Mumbai, Jun 21: Maharashtra government on Thursday said it would be mandatory for teaching and non-teaching employees in the state to possess an Aadhaar card to draw their salaries from August.

"UID number is mandatory for teaching and non-teaching employees to draw their monthly salaries," Chief Minister Prithviraj Chavan was quoted as saying in a press statement issued here.

Chavan held a review meeting on Aadhaar card registration at his residence, which was attended by UIDAI Chairman Nandan Nilekani, chief secretary of Maharashtra J K Banthia and other senior officials of the state government.

"Speedy registration procedures are on to avail the Aadhaar card. UID number is mandatory for the government employees, college students availing scholarships," Chavan said.

Nilekani expressed satisfaction over UID registration process in the state and said a report in this regard will be submitted to the central government, it said.

RTE WATCH

Kerala makes Aadhar card mandatory for RTE admissions

The Kerala government has made Aadhar cards for RTE admissions mandatory, participation in events and application for scholarship under the Kerala RTE Rules (read more). The government has decided to distribute benefits to children from disadvantaged groups on the basis of a unique identification number. The Kerala State Information Technology Mission (KSITM), along with IT@schools is organizing camps to ensure that ll students obtain Aadhar cards.

As per the Kerala RTE Rules, it is mandatory for every local authority to ensure that an Aadhar card is distributed to every child in order to maintain records. These records must be maintained transparently and must be made available in the public domain. Children's enrollment, attendance, learning assessment, and transition must be tracked within this system. Schools are also under an

obligation to maintain records of unique identification number and other biometric information of all children. In fact, such records also have an impact on the grant of recognition to schools.

It is worth asking the question – will admission be denied illegible from disadvantaged backgrounds for the want of a unique identification number? When the state has a duty to ensure completion of elementary education of every child, can the state deny admissions to children who do not possess an Aadhar card? It is also noteworthy that the rules do not mention the Aadhar Card as a document for securing admission to schools. In case a child does not have a birth certificate, the Rules allow the local authorities to consider Hospital/Anganwadi/Mid-Wife/ Auxiliary Nurse register records or an affidavit from the parents.

ONE COMMENT ON "KERALA MAKES AADHAR CARD MANDATORY FOR RTE ADMISSIONS"

My Aadhaar Card A Complete Guide to Aadhaar and Aadhaar Enrollment

Aadhaar must for Admission in Schools & Colleges

Aadhar card is now mandatory for the students to take admission in school and colleges in Himachal Pradesh. The educational department has applied this system and along with government school and colleges, private institutes also come under its realm. According to the education department the schools and colleges have to make a column for Aadhaar number in the registration and admission form. Aadharr number of each student will be recorded in this. The educational institutes have to implement this from the 2013-14 session so that at the time of entrance into the classroom the Aadhaar details of the student can be kept. Along with government and private schools, this order applies on colleges as well. Along with this the implementation will also be applied in Sanskrit colleges.

The director of education department said that the government and private educational institutes have to follow this. This decision has been taken by identifying the importance of Aadhar card. The institutes should finish the process before beginning of the session.

After the order from the central government the education department has asked for Aadhaar card from those students who take benefits from various scholarship schemes. Most of the students from schools and colleges do not have Aadhaar card due to which problems are arising in sending the details to the central government. However, since it is the first time, slackness is being seen in this. According to the rules of centre students can even be deprived of it if they do not have Aadhaar card. Such problems do not occur in the future, the department has been preparing for it already.

1. Aadhar to be used for admission in IDOL
2. Student's scholarship through Aadhaar only in HP
3. Schools to enroll students for Aadhaar in HP
4. Aadhaar for every student in Maharashtra by 2014

Aadhaar-mandatory for scholarship and fellowship

The Aadhaar card is now mandatory for college and university students who want to get scholarship and fellowship from either University Grant Commission (UGC) or the state government A UGC official said that the commission has taken a decision to link the Aadhaar number of the students with their bank accounts so that they can obtain fellowship and scholarship without any

difficulty. Universities and colleges have been asked to implement on this decision.

The UGC has asked the universities to appoint a regional officer on priority basis who will assist the students in this regard and also keep an eye on the institutes. The officer said that the Unique identification Authority of India has taken the step to provide Unique Identification (UID) number to every resident of this country which will assist in effective implementation of the welfare schemes. He said that under this initiative the decision for adding direct cash transfer with the bank accounts of the students has been taken.

He told that the appointment of such officer will be compulsory for every college affiliated with the university. The officer related with the subjects of Aadhar card and scholarship will be in coordination with the state government. UGC has sent note to universities in this regard an asked to fast forward the work ahead. The University Grant Commission has also asked the students to take initiative in the direction of obtaining their Aadhar cards. However the last date for students to obtain the Aadhar card has not been declared yet.

Under the current practice, students apply for fellowship to UGC only after getting acceptance and recognition from

the university. After that the amount is transferred into the account of the university and then students receive it through cheques.

1. Student's scholarship through Aadhaar only in HP
2. Plea against making Aadhaar mandatory in Delhi HC
3. Aadhar to be used for admission in IDOL
4. Schools to enroll students for Aadhaar in HP

Pension and PF through Aadhaar only in entire Madhya Pradesh

After receiving order from the central government, Madhya Pradesh government made Aadhar card mandatory for pension and PF from January 1 in three districts viz, Khandwa, Harda and Hoshangabad. Soon this scheme will be implemented in the entire state. According to official information EPFO notified thousands of its members from these three districts that soon this scheme will be implemented in the entire state. State government through central government's order said on Friday that Aadhaar details of all pensioners and members of EPFO will be collected and linked with bank accounts by December 31 of all the 31 districts. Officials have been asked to carry out this process by setting up camps.

UIDAI will setup permanent Aadhaar enrollment centers in the state of Andhra Pradesh within a month time. The official reports have informed that somewhere around

1400 permanent enrollment camps would be setup in all parts of the district. These centers will be in operation along with the existing Mee-Seva centers. IT Department of Andhra Pradesh will operate these camps with the support of central common service centre. Setting up of permanent centers will facilitate people for easily accessing Aadhaar services.

A report published recently in Mid Day revealed that the details collected through Aadhaar enrollment form are being leaked to third-party without knowledge of the enroller. According to the report, a Colaba-based couple got an account opening letter from a bank in the name of their 10-year-old daughter. The welcome letter from the Indian Overseas Bani (IOB) claimed that a savings Bank (SB) account has been opened in the name of the 10-year-old girl. The family is unaware about this and is shocked about their details reaching to a bank. According to the these details reached to it through central government while UIDAI clarified that nothing is forwarded to any third-party without the knowledge of the enroller.

1. Illegal enrollment camps at Politician's offices in Delhi to be seized.
2. Aadhaar enrollment soon in Banks in selected districts
3. 3.84 lakh fake Aadhaar numbers cancelled by UIDAI
4. New ATMs to be setup by the state-run Banks.

Aadhar to be made mandatory for school children

Thiruvananthapuram: A decision has been taken to complete Aadhar registration for school children within March 31. Some schools have only completed the enrollment of students and the government has appointed Keltron and IT @school to complete the enrollment process. The banks have also come forward to offer their services. From the next academic year onwards, all allowances to children will be given through Aadhar like scholarship, grant, certificates and participating in competition and will be connected through Aadhar. Children without Aadhar will not be eligible for anything.

In the order issued by the state education department, it has been made clear that the education officers and headmaster should take steps to make available Aadhar to all students. The decision was taken in the meeting led by IT department principal secretary.

THE HINDU

Published : January 24, 2013

Aadhaar cards mandatory for PF transaction

Over 50 million existing EPFO subscribers would be required to furnish their Aadhaar numbers to the body by June 30 this year. Photo P.V. Sivakumar.

Salaried employees in organized sector will have to provide their Aadhaar numbers for seeking benefits under the EPF scheme being operated by retirement fund body Employees' Provident Fund Organization (EPFO).

It will also be mandatory for new members to submit their Aadhaar numbers as part of the KYC (Know Your Customer) verification from March 1, 2013.

"It has been decided to make Aadhaar numbers mandatory for new members...joining on or after March 1, 2013. However for existing members, the seeding of Aadhaar number has to done in a time bound manner," an official order to the field staff said.

It has asked the field staff to ensure the collection of data (Aadhaar) in respect of member joining on or after March 1, 2013 on a monthly basis and in respect of existing members by June 30, 2013.

In case an employee does not have the Aadhaar number, the employer can issue an Enrolment Id (EID) as per the guidelines of the body. This EID would be converted into Aadhaar number later on, the order said.

The body would also seek the Aadhaar numbers of its pensioners through the banks. EPFO has decided to use Aadhaar as mandatory KYC credential to improve its services.

The pensioners can submit their Aadhaar number either to their pension paying branch of the bank or to the EPFO office.

The field staff has also been asked to contact the local UIDAI authorities requesting them to set up camps for enrolment in industrial areas and other places which they find suitable for the purpose.

The field offices are also directed to coordinate with district authorities during organizing of camps for Aadhaar enrolments.

Earlier, EPFO had envisaged replacing its member's account number with Aadhaar numbers to avoid inconvenience to those who had to apply for transfer of PF money to the new account with the new employer.

EPFO is working towards creating a central database where all members would have a unique account number and would not require to transfer PF accounts to another one in the event of changing jobs.

EPFO recently digitalized its database of regional offices and launched its e-passbook service where subscribers can access their account online. Now the body is working towards integrating this digital data base and bring them together at one place.

This will help EPFO members, particularly the construction workers, who often change their jobs or contractors.

Keywords: Provident Fund, Aadhaar numbers, Employees' Provident Fund Organization, EPFO, UIDAI

80

ANNEXURE - P/5 (COLLY)

dna

Coriander S/o Pulao, Aadhaar No 499118665246

Thursday, Jun 28, 2012 New Delhi

Manan Kumar

home minister asks UIDAI to get a security audit done after reports of aadhaar no given to non-entities.,

Coriander and an apple, as per the Unique Identification Authority of India (UIDAI), are residents of India as they have been given an Aadhaar number. And this, perhaps, has been the last straw.

Expressing shock at this, not to mention there having been several complaints of impersonation, the Union home ministry has asked UIDAI to get an internal as well as external security audit done by a third party to fix the lacunae in the enrolment system and avoid any more goof-ups.

The ministry had told UIDAI last month. It shot a reminder last week after seeing some more bizarre reports. If UIDAI doesn't reply, the ministry may have to seek Intelligence Bureau's (IB) help for the audit, sources told DNA.

According to a report, an Aadhaar card with the number 4991 1866 5246 was issued in the name of Mr Kothimeer (coriander), son of Mr. Palavu (pulao), resident of Mamidikaya Vuru (raw mango village) of Jambuladinne in Anantapur district of Andhra Pradesh. The card had the photo of a mobile phone instead of a person.

The ministry is in possession of about a dozen more such astonishing examples where a number has been given to non-entities.

"As the Aadhaar and NPR database are complementary to each other and are being used to enhance security and strategic processes, the ministry has the right to seek a security audit of any of its process," a ministry official said.

Overruling Chidambaram's objections on UIDAI's security, the Union cabinet on January 27 had come out with a compromise formula and given a go-ahead to the UIDAI to expand its project to 600 million people.

It was agreed that both projects will continue simultaneously and each would use the biometric data collected by the other. In case of any discrepancies, the NPR data would prevail as it is collected by government officials who are accountable.

In the same cabinet meeting, Nandan Nilekani had said, "We will review the security concerns in six to eight weeks and begin data collection from April."

"In spite of all its assurances, the UIDAI is yet to get back to us and apprise us of the changes. We have no clue what are they up to," said the official.

Business Line

Unique ID row resolved ; Authority to resume work in April after review.

NEW DELHI, JAN. 27:

The Cabinet may have brought about a truce between the Home Ministry and Planning Commission on the issue of duplication in biometric cards, but round one seems to have gone in Mr P. Chidambaram's favour.

For one, the UIDAI (Unique Identification Authority of India) will now focus only in 16 States and Union Territories where it has already started work. The rest of the country will be covered by the National Population Registry (NPR) database being collected by the Home Ministry.

'INTENSIVE REVIEW'

Following security concerns, the UIDAI will resume work only on April 1, after 'intensive review of all processes and procedures'. This was stated by Mr. Chidambaram at a press briefing here on Friday.

The Cabinet, however, sanctioned an additional Rs 5,000 crore to the UIDAI to cover 40 crore people, taking the total to 60 crore, he said.

"By doing this, most avoidable costs and duplications have been avoided. This will also speed up the process, which we hope to complete by June 2013," he said.

The Home Minister made it clear that in case of any discrepancy, the NPR data will prevail, as it is mandatory household data which capture 15 fields of information, as opposed to five by the UID, which is voluntary.

"The only minor change in the NPR's mandate is that if a person already has an Aadhaar number, his biometrics will not be captured," he added.

Terming the Cabinet's decision as the "best of both worlds", the UIDAI head, Mr Nandan Nilekani, said it combines the strengths of both the models.

aditi.n@thehindu.co.in

(This article was published on January 27, 2012)

Keywords : Home Ministry, Planning Commission, duplication, biometric cards, UIDAI, Unique Identification Authority of India, National Population Registry, NPR database,

THE HINDU

Published : December 16, 2011

Aadhaar : time to disown the idea

The government should pay heed to the parliamentary standing committee's views and suspend the Aadhaar project. It would be a travesty to push the project in through the backdoor.

"...The Committee categorically convey their unacceptability of the National Identification Authority of India Bill, 2010...The Committee would, thus, urge the Government to reconsider and review the UID scheme...."

This was the conclusion of Parliament's Standing Committee on Finance (SCoF), which examined the Bill to convert the Unique Identification Authority of India (UIDAI) into a statutory authority. With this categorical rebuff, the SCoF dealt a body blow to the Aadhaar project, which is being implemented from September 2010 without Parliament's approval.

Technically speaking, the SCoF report asked the government to bring forth fresh legislation before Parliament. However, a careful examination of the report shows that it does not just reject the Bill, it also raises serious questions about the idea of Aadhaar itself. In fact,

the report so comprehensively questions the idea that any effort to introduce fresh legislation would require, as a prerequisite, a re-look at the foundational principles on which the project was conceived.

There are broadly five important arguments in the SCoF report.

First, it contains scathing criticism of the government for beginning Aadhaar enrolment without Parliament's approval for the Bill. Currently, UIDAI enjoys only executive authority, and no statutory authority. The justification that the government presented before the SCoF was as follows: the powers of the executive are co-extensive with the legislative powers of the government, and this allows the government to exercise executive powers in spheres not regulated by legislation.

The government also cited the Attorney-General's advice, which noted that "executive power operates independently" of Parliament and that "there is nothing in law that prevents the [UIDAI] from functioning under the Executive Authorization."

The SCoF rejects this position, and states that the government's legal justification "does not satisfy the Committee." The legal position upheld by the SCoF is that

co-extensiveness of powers does not permit the executive to do what it pleases; when constitutional rights and protections are potentially violated, the powers of the executive remain circumscribed by those of the legislature.

Secondly, the SCoF raises serious questions about the enrolment process followed for Aadhaar numbers. The issue of Aadhaar numbers "is riddled with serious lacunae," and this problem can be traced to conceptualization "with no clarity of purpose" and implementation in "a directionless way with a lot of confusion." For instance, the Ministry of Finance felt that there was "lack of coordination" across the six agencies collecting personal information, leading to "duplication of efforts and expenditure." The Ministry of Home raised "serious security concerns" over the introducer model used to enrol persons without any proof of residence.

The report concludes that the enrolment process "compromises the security and confidentiality of information of Aadhaar number holders," and has "far reaching consequences for national security." The reason: "the possibility of possession of Aadhaar numbers by illegal residents through false affidavits/introducer system."

Thirdly, the SCoF comes down heavily on the government for proceeding with the project without "enactment of a national data protection law," which is a "pre-requisite for any law that deals with large-scale collection of information from individuals and its linkages across separate databases."

In its submission to the SCoF, the government had taken a dismissive view of the right to privacy of individuals. It noted that "collection of information without a privacy law in place does not violate the right to privacy of the individual." The SCoF rejects this view, and notes that in the absence of legislation for data protection, "it would be difficult to deal with the issues like access and misuse of personal information, surveillance, profiling, linking and matching of databases and securing confidentiality of information."

Fourthly, the report strongly disapproves of "the hasty manner" in which the project was cleared. It concludes that a "comprehensive feasibility study...ought to have been done before approving such an expensive scheme." This conclusion follows the government's admission to the SCoF that "no committee has been constituted to study the financial implications of the UID scheme," and that

"comparative costs of the Aadhaar number and various existing ID documents are also not available."

The total cost of the Aadhaar project would run into multiples of ten thousand crore of rupees. For just Phase 1 and 2, where 10 crore residents were to be enrolled, the allocation was Rs. 3,170 crore. For Phase 3, where another 10 crore residents are to be enrolled, the allocation is Rs. 8,861 crore. In a rough extrapolation, for 120 crore residents the total cost would then be over Rs. 72,000 crore. Is the Comptroller and Auditor General listening?

Fifthly, the report tears apart the faith placed on biometrics to prove the unique identity of individuals. It notes that "the scheme is full of uncertainty in technology" and is built upon "untested, unreliable technology." It criticises the UIDAI for disregarding (a) the warnings of its Biometrics Standards Committee about high error rates in fingerprint collection; (b) the inability of Proof of Concept studies to promise low error rates when 1.2 billion persons are enrolled; and (c) the reservations within the government on "the necessity of collection of IRIS image." The report concludes that, given the limitations of biometrics, "it is unlikely that the proposed objectives of the UID scheme could be achieved."

The SCoF report cites the experience from the United Kingdom, where a similar ID scheme was shelved. It dismisses the government's contention that "comparison between developed countries...versus India...is not a reasonable one." It states that "there are lessons from the global experience to be learnt," which the government has "ignored completely." It cites issues of cost overruns, fallacies of technology and risks to the safety of citizens, and notes: "as these findings are very much relevant and applicable to the UID scheme, they should have been seriously considered."

The SCoF report has invited sharp reactions from the business press and pro-business lobbies. One report argued that, after the Foreign Direct Investment-in-retail fiasco, it is "another Indian reform massacre;" for another, it is a "setback to the government's attempts to revive faltering economic reforms;" and for yet another, the title was "UPA reforms agenda hit again."

These predictable reactions only reaffirm the widely held belief that Aadhaar is an integral component of the neo-liberal reform programme of UPA-2. In fact, the SCoF deserves praise for standing up to pressure from powerful quarters, and not allowing the moment to be hijacked by vested interests. Ironically, till last week, the same SCoF

had come in for profuse praise from none other than Nandan Nilekani himself. He had said in August 2011: "I have had the occasion to...make a presentation on more than one occasion to the Standing Committee...let me tell you they do an extraordinarily thorough job. I am very, very impressed with the quality of questions, the homework, the due diligence, the seriousness that they view these things with. And it is very bipartisan, you can't make out who is from which party because they all ask on the issue. So when you have such an excellent system of law-making...Let us respect that, let us give them the opportunity to call all the experts for and against and let them come out with something. They are the appropriate people, they are our representatives."

The "representatives" have now spoken. For the government, the most dignified way ahead is to pay heed to the SCoF's views and suspend the Aadhaar project immediately. Each conclusion in the report should be discussed threadbare in the public domain. Biometrics should be withdrawn from government projects as a proof of identity. Alternative, and cheaper, measures to provide people with valid identity proofs should be explored. However, it would be a travesty of democratic principles if the government disregards the SCoF report and pushes the project in through the backdoor.

(R. Ramakumar is Associate Professor with the Tata Institute of Social Sciences, Mumbai)

Keywords: National Identification Authority of India Bill, UIDAI, Aadhaar scheme, Standing Committee on Finance stand.

Photo ID certificates are on sale for Rs 100

TNN Nov 1, 2011

BANGALORE : A well-oiled network of touts and government officials is cashing in on the people's yearning to have an Aadhaar number, which is slated to become mandatory to avail a slew of government services.

Serpentine queues are seen in front of Jayanagar General Hospital, Tilaknagar, over the past week as people are flocking to the doctors there to obtain photo identity certificates. Every individual keen on obtaining the certificate is coughing up Rs 100 for it. A photo identity certificate issued by a Group A gazette officer is among the identity documents prescribed for obtaining Unique identification numbers.

All this hospital, Aadhaar business is thriving. A doctor identified as Sridhar ST, senior specialist in the rank of district surgeon, is allegedly signing away identity

certificates without even checking to whom and what he is certifying. An enterprising Jayanagar resident, Mir Saifullha, decided to carry out a sting operation and expose how identities were at stake in the photo ID certificate racket.

"I pasted only my photo on the identification certificate form and left the rest blank. Yet, the doctor affixed his seal and signed on the photo, certifying that I am resident of the unstated address for five years and he knew me. He did not check why I had to pay Rs. 100 to an agent who promised the certificate would get me an Aadhaar card ", said Mr.Saifullah.

94

ANNEXURE-P/6

Photo ID certificates are on sale for Rs 100

TNN Nov 1, 2011, 03.05 AM IST

BANGALORE: A well-oiled network of touts and government officials is cashing in on the people's yearning to have an Aadhaar number, which is slated to become mandatory to avail a slew of government services. Serpentine queues are seen in front of Jayanagar General Hospital, Tilaknagar, over the past week as people are flocking to the doctors there to obtain photo identity certificates. Every individual keen on obtaining the certificate is coughing up Rs 100 for it. A photo identity certificate issued by a Group A gazetted officer is among the identity documents prescribed for obtaining Unique Identification numbers. At this hospital, the Aadhaar business is thriving. A doctor identified as Sridhar ST, senior specialist in the rank of district surgeon, is allegedly signing away identity certificates without even checking to whom and what he is certifying. An enterprising Jayanagar resident, Mir Saifullah, decided to carry out a sting operation and expose how identities were at stake in the photo ID certificate racket."I pasted only my photo on the identification certificate form and left the rest blank. Yet, the doctor affixed his seal and signed on the photo, certifying that I am resident of the unstated address for five years and he knew me. He did not check why I had to pay Rs 100 to an agent who promised the certificate would get me an Aadhaar card," said Mir Saifullah.

ANNEXURE - P/7

UNIQUE INDENTIFICATION AUTHORITY OF INDIA

PLANNING COMMISSION

GOVERNMENT OF INDIA

3rd Floor, Tower-II, Jeevan Bharati Building,

Connaught Circus, New Delhi - 110 001

NOTICE INVITING APPLICATIONS FOR HIRING OF BIOMETRICS CONSULTANT

(A-11016/07/10-UIDAI)

The Unique Identification Authority of India (UIDAI) invites applications from experienced individual professional consultants working in the area of Biometrics for assisting in proof of concept of Biometric solutions for UIDAI project. The duration of consultancy assignment would be for six months beginning March'2010.

For the details of qualifications and list of deliverables, applicant may see www.uidai.gov.in with subject 'Hiring of Biometric Consultant' (under Tenders section).

The applications with CV should reach the Deputy Director General , UIDAI, 3rdFloor Tower-II Jeevan Bharati Building, New Delhi - 110001 and/or may be emailed to ddguidai@gmail.com with subject 'Hiring of Biometric consultant' on or before 23th February 2010.

All queries and clarifications should be addressed to: 'Deputy Director General, UIDAI, 3rd Floor Tower-II Jeevan Bharati Building, Connaught Circus, New Delhi; Tele/Fax: 011- 23752671,23753706.

Sd/- B.B.Nanawati
Deputy Director General
UIDAI, New Delhi

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

PLANNING COMMISSION

GOVERNMENT OF INDIA

3rd Floor, Tower-II, Jeevan Bharati Building,

Connaught Circus, New Delhi - 110 001

F.No. A-11016/07/09-UIDAI

Hiring of Biometric Consultant for UIDAI

[For assisting in POC of Biometric Solutions]

Qualifications :Biometrics Consultant

- Doctorate in biometric technology from international university recognized for outstanding biometric work
- Actively involved in research and must have authored numerous research papers and books on biometric technology
- Hands on experience in biometric matching algorithm including original contribution in the same
- 5+ years of experience as chief scientist or CTO in a biometric company or equivalent role in the consulting company.

- Hands on experience in designing and evaluating different algorithms at mathematical/internal level

Deliverables

1. Build biometric component of enrollment workstation software including automated quality check and enhancement tools for PoC.

The success of the UID project depends on the accuracy of biometric de-duplication to ensure that one person can obtain only one UID number. The most significant factor contributing to the accuracy of biometric de-duplication is the quality of acquired biometric data. Many factors affect quality of biometric data. The most important factor affecting quality of capture is capture process, quality feedback, and quality of capture devices.

The capture process is a combination of logistics of biometric data acquisition, ergonomic considerations (e.g., should the subject be standing or sitting etc.), sequence of actions for the operator, sequence of actions for the subject, the ease of use of the capture

software, and type of quality feedback, capture sequence, etc. The capture software should be intuitive, easy to use, and assist in capture process in such a way as to maximize the quality of captured biometric data as well as throughput.

UIDAI needs high quality design and implementation of capture software as well as process that maximizes the quality of captured biometric data in the Indian context. For the western world, NIST for instance has invested tens of man-years of work to come up with recommendations for biometric capture process. See http:// zing. ncsl.nist. gov / biousa/. Studies conducted by NIST have included usability of height and angles of ten-print fingerprint capture, types of instructions provided to the subject, effect of scanner/table height on the fingerprint capture, health and safety perception of biometric devices, effects of habituation to biometric devices etc. UIDAI requires design and development of capture software that is appropriate for the Indian context as well as a detailed process flow that is adapted to rural India. Also, specific considerations need to be made for the particular application of the UID in India.

The Consultant will generate a reference design and implementation of biometric capture software and process be studied, developed, and delivered to UIDAI in source code. The reference implementation will designed such that biometric device from different vendors can be integrated easily.

2. Design biometric PoC to test key hypothesis (list hypothesis and importance of hypothesis) and to use for benchmarking during pilot biometric vendor selection.

There are two objectives of the UIDAI biometric PoC. The first objective is to assess the biometric de-duplication accuracy that can be achieved in the Indian context. NIST has spent considerable efforts over the past 10-15 years in benchmarking the state-of-the-art extractor and matching technology for fingerprint, face, and iris biometrics on the western population. See http://fingerprint.nist.gov/, http://face.nist.gov/, and http://iris.nist.gov/. While NIST documents the fact that the accuracy of biometric matching is extremely dependent of 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 climates and facilities without air-conditioning). In fact we could not find any credible study assessing the achievable accuracy in any of the developing countries. UIDAI has performed some preliminary assessment of quality of fingerprint data from Indian rural demographics and environments and the results are encouraging. The "quality" assessment 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 of the biometric data – each biometric (fingerprint and iris) on its own as well as in a combination.

The second objective of PoC is to collect biometric data to be used in benchmarking biometric de-duplication technology and software. Such a benchmark will be critical in vendor selection. Biometric de-duplication technology is a complex technology that requires several evaluation criteria to be assessed simultaneously. For example, false positive

identification rate (FPIR) and false negative identification (FNIR) rate as well as the change in these error rates as related to number of identities in the gallery. Further, the matching speed is related to the error rates as well as number of identities in the gallery. NIST has conducted a large number of vendor comparisons over the past two decades. However there are two problems in using NIST evaluations for UIDAI. Firstly, NIST has not conducted the evaluation with the UIDAI application in mind, for example, NIST does not benchmark matching speed together with matching accuracy. Secondly, the benchmarks are a snapshot in time while the technology evolves over a period of time. As a result, many of the NIST benchmarks can are outdated. And finally, NIST has not benchmarked fusion of the biometrics relevant to UIDAI.

The Consultant will specify key hypothesis should be tested to understand the achievable accuracy from biometrics on Indian demographics and conditions. The Consultant will design PoC process to collect necessary data to test the hypothesis. The design

should be statistically valid and accurate to achieve stated goals.

3. During PoC sample and monitor software and process to suggest improvements in the process.

The UIDAI PoC will commence with biometric enrollment capture software as specified/required above. As the PoC progresses in the field, the operation of capture software and process will need to be monitored. Such monitoring is required to fine tune the software and process to make it as efficient as possible. Example may include a change in the sequence of biometric data capture, a change in the physical setup of the capture stations, a change in the instructions provided to subjects, or a fine tuning of parameters in the capture software may result in a more efficient and more effective process. Efficiency in biometric data capture can result in huge cost savings when the UIDAI program scales to a large population. The capture software and process also needs monitoring to fine tune the quality of biometric capture. It is well known that the quality of captured biometric data is the most important factor contributing to the de-duplication accuracy. The

captured biometric data from the PoC is required to be monitored to fine tune the software and process.

The Consultant will visit PoC fields sites, review the operation, make observation, suggest improvement and provide final report stating level of conformance with the designed plan. The Consultant will provide in writing report on recommended changes for the remaining PoC process.

4. Design analytical models and process for calculating accuracy and performance of different biometric traits as well as fusion of multiple traits from the PoC data.

Evaluation of biometric technology is a complex task not only due to the fact that it needs to be evaluated on a number of parameters but also due to the fact that the evaluation is statistical in nature. The results may not be repeatable if there are even slight changes in any parameters. UIDAI requires design of analytical framework to specify which types of tests are to be conducted and how to assess if the test results are statistically significant. UIDAI requires design of experiments to assess how to combine the biometrics used in the UIDAI application (10 fingerprints, 2 iris, and face) to achieve the correct balance among

throughput, cost, and the matching accuracy. If not carefully assessed and evaluated, UIDAI may procure software that is more expensive, requires a larger data center, and yet not very accurate. This balance of accuracy and performance is very delicate and UIDAI application specific.

The Consultant will provide detailed methodology and process for calculating accuracy and performance for each biometric modality separately as well as different applicable combination (fusion) of modalities for PoC.

5. Review biometric operational best practices document for urban and rural environment including enrollment sequencing and monitoring to result in highest quality of capture.

As mentioned above, UIDAI requires initial enrollment capture software and process design and implementation for the PoC. Fine tuning of the software and process will occur during the data capture of the PoC. After the PoC, the capture software and process will need to be updated and generalized for the UIDAI Pilot. This is due to the fact that post-PoC, the software and process will be required to be more generic. For example, different

process may be followed in rural locations than in urban locations. Slightly different processes may be required in different states. While process must be adapted to be more generic, the process should still acquire the best possible biometric data. UIDAI requires expert review of the operational best practices document for urban and rural environment. This review will include the software used for biometric data capture, devices used for the capture, as well as the process followed. The review will be conducted through an examination of the biometric data collected from the field.

The Consultant will review final PoC result documents for accuracy, completeness and best practice recommendations. The Consultant will review final software and provide written report on suggested enhancements for Pilot phase.

6. Develop biometric technology requirements to be given to PMC for MSP tender

The PMC is responsible for writing tender to select Managed Service Provider. The specific requirements for biometric enrollment, de-duplication and authentication server need specialized knowledge of

biometric algorithms, image processing techniques and statistical tools. The requirements will also cover integration of biometric solution with the remaining UID. This integration must be done in a way to avoid vendor lock-in, utilize opens source technology to the extent possible and support e-governance cloud architecture. Each component of biometric solution should be modular and would allow for its replacement without affecting remaining components. The requirements will also include models for balancing accuracy against resource requirements (H/W) and dynamically changing matching algorithm threshold as the database size increases. Finally, the requirements must meet UID Biometric ,Standards and other international standards. The Consultant will provde comprehensive requirements to the PMC to be included in the MSP tender. The requirements will include the design of the system as well as the biometric technology requirements and judgment criteria.

7. Develop biometric de-duplication design for pilot and support integration needs of the Pilot software development team.

The UIDAI technology team will develop UID Pilot software. The Pilot software will integrate biometric de-duplication software from short listed biometric solution vendor. UIDAI requires the design of biometric software into the Pilot software such that multiple biometric vendor solution can be easily integrated and operated in parallel. The overall design should be robust, general, scalable, and avoid vendor/technology lock-in. It should be standards-based and quality conscious.

The Consultant will generate a document containing the design of the biometric component for the UIDAI Pilot as well as providing support for the integration of biometric technology into the Pilot software. The integration may combine different biometric technologies from different vendors. The integration design must achieve the right balance among accuracy, speed, and cost of software and computational resources (data center).

8. Design benchmarking requirements and benchmarking process for evaluating vendor solution during Pilot

During the tender evaluation process (concurrent with Pilot), the specific proposals of the biometric vendors will be required to be benchmarked and evaluated. Such an evaluation will consider biometric de-duplication accuracy, matching speed, and cost of the software and computational resources. UIDAI needs requirements for vendor in terms of deliverables from the vendors. UIDAI also needs requirements and process for evaluating the vendors on biometric technology as well as integration. The benchmarking protocols must be representative of the UIDAI application. For example, under the patriot act, NIST performed many large benchmarks between 2002 and 2006 for the specific application of border control in the US. See http://www.itl. nist.gov/iad/ 894.03/ pact/pact.html. Such efforts are required for the specific application of UIDAI. The design of benchmarking and benchmarking process for evaluating solution during vendor selection is required by UIDAI to be performed diligently. The database during pilot will remain small compared to the eventual target of 1.2B. The benchmarking may consist of synthetically generating biometric samples or collecting data from pre-existing databases of the

various GoI departments and agencies. The benchmarking will incorporate several variables: database size, accuracy, resource requirements and performance. Therefore the benchmarking protocol must be designed scientifically to meet UIDAI's goals.

The Consultant will in conjunction with UIDAI Pilot team will develop benchmarking requirements and process for vendor evaluation.

9. Evaluate benchmarking results and provide comparative benchmark assessment

Once the benchmarking is performed as per the design that will result from the point above, the results will be required to be analyzed and interpreted. As mentioned before, biometric evaluations are multi-dimensional. And more importantly the biometric evaluations are statistical. The statistical significance of the test results are required to be analyzed for UIDAI.

The Consultant will develop framework for collecting benchmark results and analyzing the final data. The Consultant will review the results and provide his interpretation of the results. Finally, the Consultant

will recommend the biometrics solution based on the benchmarks.

112

ANNEXURE - P/8

Template Aging in Iris Biometrics: Evidence of Increased False Reject Rate in ICE 2006

Sarah E. Baker, Kevin W. Bowyer, Patrick J. Flynn and P. Jonathon Phillips

Abstract Using a data set with approximately four years of elapsed time between the earliest and most recent images of an iris (23 subjects, 46 irises, 6,797 images), we investigate template aging for iris biometrics. We compare the match and non-match distributions for short-time-lapse image pairs, acquired with no more than 120 days of time lapse between them, to the distributions for long-time-lapse image pairs, with at least 1,200 days of time lapse. We find no substantial difference in the non-match, or impostor, distribution between the short-time-lapse and the long-time-lapse data. We do find a difference in the match, or authentic, distributions. For the image dataset and iris biometric systems used in this work, the false reject rate increases by about 50% or greater for the long-time-lapse data relative to the short-time-lapse data. The magnitude

of the increase in the false reject rate varies with changes in the decision threshold, and with different matching algorithms. Our results demonstrate that iris biometrics is subject to a template aging effect.

1 Introduction

The term "template aging" refers to degradation of biometric performance that occurs with increased time between the acquisition of an enrollment image and acquisition of the image compared to the enrollment. Template aging effects are known to exist for biometrics such as face and fingerprint [7][28][31][19][27].

The iris biometrics community has long accepted the premise that the iris is "essentially stable" throughout a person's life, and that this means that template aging does not occur for iris biometrics. Daugman stated the core assumption this way- "As an internal (yet externally visible) organ of the eye, the iris is well protected and stable over time" [8]. This assumption is commonly repeated in research publications dealing with iris biometrics: "[the iris is]

stable over an individual's lifetime"[30], "[the iris is] essentially stable over a lifetime"[22], "the iris is highly stable over a person's lifetime"[24]. The commercial iris biometrics literature explicitly connects this to the idea of lifetime enrollment - "only a single enrollment in a lifetime"[17].

Note that claims about stability of the iris texture and "lifetime enrollment" are never presented as dependent on the particular sensor, algorithm, length of time lapse or any other condition. They are presented as universal claims about iris biometrics in general. Thus a single counter-example is sufficient to disprove the universal claim.

It is well known in the medical literature that the eye and iris undergo a variety of changes with age [2][5][12][23][33][34]. Any of these effects could in principle alter details of the imaged iris texture. It is also possible that a tempate aging effect could be due to aging of the sensor, changes in how a person uses the biometric system, or other factors. The essential question for iris biometrics is - does the quality of a

match between two images of the same iris change with increased time between the enrollment image and the image to be recognized? That is, does a template aging effect exist? We present results of the first systematic investigation of this question.

We use an image dataset involving 23 persons (46 irises) with approximately four years of time lapse between the earliest and latest images of a given iris. We consider image pairs in a short-time-lapse group, representing no more than 120 days of time lapse between the two images, and in a long-time-lapse group, representing at least 1,200 days of time lapse. We experiment with three iris biometric systems: our medication of the IrisBEE baseline matcher [26], Neurotechnology's VeriEye system [32], and the Cam-2 submission to the Iris Challenge Evaluation 2006 [25]. We find that, for each of the three systems, there is no significant difference in the non-match, or "impostor", distributions between the short-time-lapse and the long-time-lapse data. We also find that, for each of the three systems, the match distribution

for the long-time-lapse data is different from that for the short-time-lapse data in a way that results in an increased false reject rate. Thus, we observe clear evidence of a template aging effect for iris biometrics.

2 Previous and Related Work

We do not know of any experimental study that supports the conclusion that template aging does not occur for iris biometrics. Claims about the stability of iris texture appear to be based on subjective human visual perception of iris texture visible-light images of the iris. However, it has been shown that humans are able to perceive similarities in iris texture that do not result in closer iris biometric matches [15]. Thus human perception of the general iris texture pattern does not automatically or necessarily imply anything about iris biometric operation.

Gonzalez et al. [29] report an effect of time lapse on iris recognition that may initially seem similar to our results. However, Gonzalez et al. compare matches between images acquired at the same acquisition session with those acquired with at most

three months time lapse. They report a better match statistic for images from the same session than for those across sessions. However, they show little change in match statistics when comparing matches with short time lapses, between two weeks and three months. In our results presented here, we do not consider matches between images acquired in the same acquisition session, as we expect that this is not representative of a real-world biometric scenario. We expect that "same session" images will generally result in atypically good matches. Like Gonzalez et al., we do not find any significant difference in match scores for images with a few months time lapse. However, when considering a longer time lapse than that examined in Gonzalez et al., we do observe a statistically significant degradation in match scores.

This paper expands upon our initial results [4] in several ways. First, we have increased the number of subjects from 13 to 23 and the number of irises from 26 to 46. Second, in [4] we only considered images from spring 2004 and spring 2008 and the

matches within one semester and matches across the four years. In this work we now consider all images acquired from 2004 through 2008 and have set two time thresholds in defining our short-time-lapse and long-time-lapse matches. Third, we have tested the time-lapse effect on two additional iris biometric algorithms: Neurotechnology's VeriEye [32] and the Cam-2 submission to the Iris Challenge Evaluation 2006 from the University of Cambridge [25]. We also test for various possible causes of match score degradation with increased time lapse. Finally, we present ROC curves for short-time-lapse and long-time-lapse matches for each of the three algorithms, and explicitly show the difference in the false reject rates.

3 Image Dataset and Algorithms

All of the iris images used in this study were acquired with the same LG 2200 iris imaging system [16], located in the same studio throughout the four years of image acquisition. The system had no hardware or software modifications during the four

years. The LG 2200 model is now discontinued. However, current state-of-the-art iris imaging systems of course did not exist at the time that data acquisition for this experiment started. We are currently pursuing additional work with images acquired using a newer model sensor and initial results [9] are generally consistent with results of this study.

Image acquisition sessions were held at multiple times in each academic semester across the four years. At a given acquisition session, for a given subject, six images were acquired of each eye. The image acquisition protocol was the same as that Sarah E. Baker, Kevin W. Bowyer, Patrick J. Flynn and P. Jonathon Phillips used in the Iris Challenge Evaluation (ICE) 2005 and 2006 [25][26]. However, it is important to note that while the protocol for the ICE acquisitions allowed for some images that did not pass the normal built-in quality control checks of the LG 2200 [25], all images used in this study were manually screened for image quality. Images of

noticeably poor quality were excluded from this study; e.g., out-of-focus irises, major portions of the iris occluded, obvious interlace artifacts, etc., were all excluded. Also, images that resulted in a noticeably poor iris segmentation by the IrisBEE algorithm were excluded from the study. (The detailed segmentation was not available from the other systems.)

A total of 23 persons participated in data acquisitions from 2004 through 2008. See Figure 1 for examples of iris images. There are images from both irises of the 23 subjects over the four years. Subject age ranges from 22 to 56 years old at the end of the four-year period. Sixteen subjects are male and seven are female. Sixteen subjects are Caucasian and seven are Asian. The repeated sixteen by seven break-down is a coincidence; the ethnicity division does not follow the gender division. None of the subjects wore glasses for any of the data acquisition. Five subjects wore contact lenses at all acquisition sessions, and eighteen subjects did not wear contact

lenses at any acquisition session. The total number of iris images selected for use in this study was 6,797.

We created two sets of image pairs, a short-time-lapse set and a long-time-lapse set. The short-time-lapse set consists of image pairs where the two images were acquired with no more than 120 days of time lapse between them. The average time lapse in this group is 44 days. The long-time-lapse set consists of image pairs acquired with no less than 1,200 days of time lapse. The average time lapse in this group is 1,405 days. A given iris image can participate in multiple short-time-lapse pairs and multiple long-time-lapse pairs.

4 Iris Matching Algorithms

To investigate the generality of any observed effects, three different iris biometric algorithms were included in the study. First, we used our own modified version of the IrisBEE system distributed through the ICE program [25]. This system represents an iris as a 240x10x2-bit iris code

generated from the complex-valued responses of one-dimensional log-Gabor wavelet filters applied to the normalized iris image [20]. For the IrisBEE matcher, the output of matching two iris images is a fractional Hamming distance. The range of the fractional Hamming distance is [0, 1], with zero being a perfect match and 0:5 a random level of match. Second, we used the commercial VeriEye 2.2 Iris SDK from Neuro Technology [32]. This system produces match scores on a different scale and with a different polarity than systems employing fractional Hamming distance. For the analysis in this paper, we negated the match scores so that lower scores represented better matches. The third system was the Cam-2 submission to the ICE 2006 from the University of Cambridge [25]. The output of the Cam-2 matcher is nominally a fractional Hamming distance. Thus we have used three different algorithms. One is based on a "baseline" source code that was made available to the research community, one is a readily available commercial product, and one was a best performer in the ICE 2006 results.

123

5 False Reject Rates for Short and Long Time Lapse

We computed the authentic and impostor distributions for each of the three algorithms. The impostor distributions showed no apparent difference between the short-time-lapse data and the long-time-lapse data. However, the authentic distributions for long-time-lapse data were shifted in the direction of the impostor distribution. For each of the three algorithms, the shift in the authentic distribution is such that it causes an increase in the False Reject Rate (FRR) for any practical choice of decision threshold.

Graphs that zoom in on the "tails" of the long-time-lapse and short-time-lapse authentic distributions for each algorithm are shown in Figure 2. These graphs show the tails of the distributions across a range of possible values for the decision threshold. Recall that for the IrisBEE, and Cam-2 algorithms, a smaller value (of fractional Hamming

distance) represents a better match, while for the VeriEye algorithm a larger value of different units represents a better match.

This figure shows that for all three algorithms, across a broad range of possible threshold values, the long-time-lapse authentic distribution has a higher false reject rate than the short-time-lapse authentic distribution. The IrisBEE algorithm shows approximately 150% increase in the false reject rate across the range of decision thresholds, the VeriEye algorithm shows an approximately 70% increase, and the Cam-2 algorithm shows an approximately 40% increase. Thus we observe clear and consistent evidence of a template aging effect for each of three algorithms considered in this study.

6 Frequency of Authentic Distribution With Worse Mean Score

We also performed a one-sided sign test to check for statistical significance of the frequency, across the 46 irises, of the long-time-lapse authentic distribution having a worse mean match score than

the short-time-lapse authentic distribution. A worse mean score is one closer to the impostor distribution. If time lapse has no effect, then we would expect that the long-time-lapse mean is worse for half of the irises and the short-time-lapse mean is worse for half. This is the null hypothesis for the test. The sign test does not make any distributional assumptions about the means of similarity scores. The one-sided test was selected because we are interested in the alternative hypothesis that the longer-time-lapse data has a larger mean score.

Table 1 Sign test for frequency of worse mean match score with longer time lapse.

Algorithm	No. irises	test statistic	p-value
IrisBEE	42	5.75	$2{:}55\text{x}10^{-9}$
VeriEye	41	5.46	$2{:}20\text{x}10^{-8}$
Cam-2	38	4.57	$4{:}62\text{x}10^{-6}$

The sign test results are presented in Table 1, including the test statistic, p-value, and number of irises for which the mean of the long-time match scores is worse than the mean of the short-time-lapse

match scores (ul(i)> us(i)). The results show that we can easily reject the null hypothesis for all three algorithms. The frequency of a worse match score occurring for the long-time-lapse is statistically significant. This indicates that the increased FRR seen in Figure 2 is not the result of a small number of unusual irises in the data set, but is characteristic of the data set in general.

Table 1 shows that for IrisBEE there are 42 of 46 irises for which the long-time-lapse mean HD is worse, for VeriEye there are 41 irises for which the long-time-lapse mean match score is worse, and for Cam-2 there are 38 irises for which the long-time-lapse mean HD is worse. One natural question is: how many of these irises are in common? The answers are presented in Table 2, which shows the num-ber of irises in common. The last row reports that 34 irises have the time-lapse Template Aging in

Iris Biometrics

0.25 0.30 0.35 0.40

0.00 0.01 0.02 0.03 0.04 0.05 0.06 0.07

FRR for IrisBEE

Hamming Distance

Rate

Short-time-lapse

Long-time-lapse

10 20 30 40 50 60 70 80

0.000 0.002 0.004 0.006 0.008 0.010 0.012

FRR for VeriEye

Match Score

Rate

Short-time-lapse

Long-time-lapse

0.25 0.30 0.35 0.40

0.015 0.020 0.025 0.030 0.035

FRR for Cam-2

Match Score

Rate

Short-time-lapse

Long-time-lapse

Fig.2 Authentic distributions across a range of match scores, showing increased false reject rates.

Table 2 Overlap in number of irises for which the mean of the long-time match scores is greater than the mean for the short-time match scores. The

overlap is reported for all combinations of the three algorithms and for all three algorithms.

Algorithms	N of 46 irises in common
IrisBEE-veriEye	38
IrisBEE-Cam2	35
VeriEye-Cam2	35
All three	34

effect for all three algorithms. A one-sided sign test for 34 of 46 irises showing an effect across all three algorithms produces a test statistic of 3.391 with a p-value of $8{:}207\text{x}10^{-4}$. Thus, even if we use the criteria that all three algorithms must agree on the movement of the means, the null hypothesis is rejected.

7 Possible Causes of an Increased False Reject Rate

We considered a variety of factors that could conceivably contribute to causing the observed result. For example, it is known that the presence of contact lenses can adversely affect match quality [3]. If the short-time-lapse data contained image pairs

where a subject did not wear contact lenses and the long-time-lapse data contained image pairs where the same subject was wore contacts, this could conceivably cause an increased FRR for long-time-lapse relative to short-time-lapse. Similarly, if a person was wearing the same type of contacts in short-time-lapse image pairs, but a different type in long-time-lapse image pairs, this could conceivably cause an increased FRR.

We manually checked for the presence of contact lenses in all images included in this study. We found that each subject in this study either wore contacts for all acquisition sessions, or did not wear contacts to any acquisition session. Also, for the subjects who wore contacts, none appear to have changed the type of contacts worn. Thus we conclude that the wearing of contact lenses is not an appreciable factor in our observed results.

Hollingsworth et al. [13] showed that the degree of the pupil dilation, and the difference in pupil dilation between two images, can affect the match

distribution. We performed an analysis of the changes in pupil dilation and its possible effect on the difference between long-time-lapse and short-time-lapse data.

The first step in the analysis was to compute the ratio of the pupil diameter to the iris diameter for each image. The second step was to compute the difference in the pupil-to-iris ratio for the iris images in each match pair. Then, for each subject, we computed the average change in the pupil-to-iris ratio over all short-time-lapse match pairs. We denote this by Ps(i). Similarly, we computed the average change in the pupil-to-iris ratio for all long-time match pairs, denoted by PL(i). Then for each iris, we computed the difference between the average short-time-lapse change in the pupil to iris ratio and the average long-time-lapse change in the pupil to iris ratio, denoted by rL(i) rS(i). For the IrisBEE algorithm, we created a scatter plot of the change in the pupil-to-iris ratio between long-time-lapse and short-time-lapse match pairs and change in match

score between long-time-lapse and short-time-lapse. Figure 3 is a scatter plot of Ul(i) - Us(i) versus PL(i) PsS(i). The corre- sponding Kendall correlation coefficient is 0.217. If the observed increase in false reject rate could be attributed to a change in pupil dilation, then Ul(i) -Us(i) versus PL(i)-Ps (i) would be substantially correlated. If PL(i)j –us (i) PLs(i)j, then there is a greater difference in diameters of the pupils for long-time match pairs than for short-time match pairs. In turn this implies that match scores should degrade. However, our analysis shows minimal correlation between ULL(i) -Us(i) versus PrL(i)-rPS(i). Thus we conclude changes in pupil dilation are not an appreciable factor in our observed result.

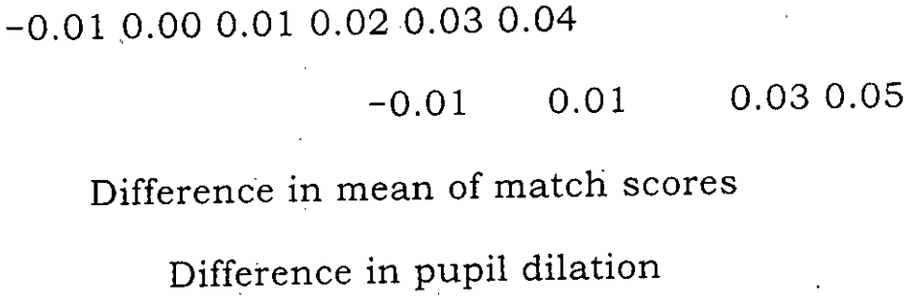

Fig. 3 Scatterplot of the change in match score between long-time and short-time lapse for each ris versus the change in the pupil to iris ratio between

long-time and short-time lapse match pairs U(i) mS(i) versus Ps(i)-Ps(i). The horizontal axis is the change in mean match scores for the ong-time and short time lapse iris pairs. The vertical axis is the change in the average short-time change in the pupil to iris ratio and the average long-time change in the pupil to iris ratio. Each red circle is an iris.

The percentage of an iris that is occluded can affect iris matching performance [10]. The more of the iris that is observable, the better the expected performance. Thus one possible factor contributing to the observed increase in the false reject rate is that the percentage of the iris that is observable decreased in the long time-lapse data relative to the short-time-lapse data.

In the IrisBEE algorithm [25], the fraction of the iris that is visible is indicated by the fraction of the iris code bits that are marked in the iris code mask as representing non-occluded portions of the iris. To determine if there is a change over time in the fraction of the iris that is occluded, we divided the

time period over which the data was collected for this study into 30-day intervals. We computed the average number of bits marked as non-occluded in the mask for all images collected in each 30-day interval. We then computed Kendall's correlation coefficient between the average number of bits marked as non-occluded and time. The resulting Kendall's correlation coefficient is -0.131. This indicates that there is no substantial correlation between number of bits marked as non-occluded and elapsed time. Thus, we conclude that change in the amount of iris occluded does not account for the increase in the false reject rate observed in our results.

The iris images in the time-lapse study were collected with the same LG 2200 sensor [16]. It is conceivable that the sensor properties of the LG 2200 could have changed over time in such a way as to cause an increased false reject rate in the long-time-lapse data. To test for this, in the Fall 2008 we collected iris images with a second rarely-used LG 2200 camera. We collected approximately 3000

images from 77 subjects (154 irises) who attended three separate acquisition sessions (labeled "session one," "session two," and "section three"). There was approximately two weeks elapsed time between each session. During sessions one and three, iris images were collected with the original camera; during session two the iris images were collected with the second rarely-used camera. The first step in our sensor aging analysis was to compute the match and non-match score distributions between iris images collected in session one and session three, both sessions using the original sensor. The second step was to compute the match and non-match score distributions between iris images collected in session one and session two. In session two, the images were collected with the second rarely-used sensor. If the sensor age affects match quality, we would expect a significant degradation in match scores between images collected from the two different sensors compared to image pairs collected with the original sensor. The average match score for image pairs collected with the original sensor is 0.215; the

average match score for image pairs collected with the two different sensors was 0.217. Figure 4 shows a histogram for the match and non-match distributions for both within and between sensor comparisons. Based on this analysis, we conclude that a sensor aging effect cannot account for the increase in false reject rate that is seen in our results.

The LG 2200 camera actively illuminates the iris using three infrared light emitting diodes (LED) positioned on the left, right, and top of the sensor. When acquiring images, the camera is designed to take three images, one with each LED. In commercial applications, the camera will save the best quality image and discard the other two. For our acquisitions, the system had the capability to save all three images (for a detailed explanation see Phillips et al. [26, 25]). It is conceivable that if there were more matches between images acquired with the same LED in the short-time-lapse group, and more matches between images acquired with different LEDs in the long-time-lapse group, that this could

result in an increased false reject rate for the long-time-lapse group.

We grouped the matches into those in which the two images were taken with the same LED and those in which the two images were taken with different LEDs. For both groups, we observed an increased false reject rate of about 50% across all feasible decision threshold values for the long-time-lapse data over the short-time-

0.00
0.05
0.10
0.15
0.20
0.25
Density
Ham

Fig. 4 The match and non-match distributions for the within and between sensors experiments. The match and non-match distributions are for the Hamming distance from the IrisBEE algorithm. The mean Hamming distance for match scores collected with the same sensor is 0.2153 and for match scores

collected with difference sensors is 0.2167. The mean Hamming distance for non-match scores collected with the same sensor is 0.4483 and for non-match scores collected with difference sensors is 0.4478.

lapse data. Thus we conclude that variations in the particular LED illuminating the images is not the cause of the increased false reject rate seen in our results.

8 Conclusions and Discussion

For three different matching algorithms, and across the range of practical decision threshold values for each matching algorithm, we found that the false reject rate increases with longer time lapse between enrollment and verification. This is seen clearly in the difference in the tails of the authentic distributions. Also, the frequency of irises with a worse mean match score for long-time-lapse compared to short-time-lapse is statistically significant. Thus our experimental results show clear and consistent evidence of a template aging effect for iris biometrics. The magnitude of the template aging

effect varies between algorithms, with the value of the decision threshold, and other factors.

We were able to test for a variety of factors that could potentially contribute to observing an increased false reject rate with increased time lapse. We concluded that factors such as varying pupil dilation, wearing of contact lenses, differences in amount of iris occluded, and sensor aging are not an appreciable factor in our experimental results.

It is possible that the template aging effect observed in our experimental results is caused by normal aging of the eye. One well-known example of age-related change in the normal eye involves pupil size. Winn et al. studied factors affecting light-adapted pupil size and found that "of the factors investigated, only chronological age had a significant effect on the size of the pupil"[33]. They concluded "the results of this study are consistent with previous reports suggesting that pupil size becomes smaller in an almost linear manner with increasing age" [33]. The iris, of course, controls the pupil size, and so

this change in average pupil size reflects a change in the functioning of the iris tissue. As the Merck Manual of Geriatrics describes it, "The iris comprises two sets of muscles that work together to regulate papillary size and reaction to light. With aging, these muscles weaken and the pupil becomes smaller (more miotic), reacts more sluggishly to light, and dilates more slowly in the dark" [23].

There are also age-related changes in the melanocytes, the cells that produce melanin, in the iris. Eye color is largely determined by the melanocytes in the anterior layer of the iris. For some segments of the population, aging can lead to a noticeable change in the melanocytes, and so the eye color. Bito et al. report that "Most individuals had stable eye color after early childhood. However, there was a subpopulation of white subjects with eye color changes past childhood. Approximately 17% of twins and 11% of mothers experienced a change in eye color of 2 U or more. [...] Thus, eye color, and hence, iridial pigmentation, seems to change in some

individuals during later years" [5]. They found that the changes in eye color were more similar for identical twins than fraternal twins, indicating a genetic link to this particular element of aging. One element of melanocyte aging can, in rare cases, lead to a cancer. "The melanocytes in the iris are constantly exposed to UV radiation, and this leads to the malignant transformation of these cells to form a specific type of malignant tumor, the uveal melanoma" [12].

Also connected with the melanocytes, iris freckles and nevi can arise in the iris, and can grow over time. "Iris freckles are the most common iris tumors found in children as well as adults. They are collections of benign, but abnormal melanocytes that vary in size and shape. Although congenital, they tend to become more prominently pigmented with age. Iris freckles are clusters of normal melanocytes and have no malignant potential. Nevi efface the iris architecture and may cause clinical structural alterations ..." [34].

In addition, it is known that the cornea undergoes age-related changes. "The shape and aberrations of the cornea change with age. It is well known that the radius of curvature slightly decreases with age, and the asphericity also changes. On average, the cornea becomes more spherical with age and, as a consequence, spherical aberrations tend to increase" [1]. The iris is imaged through the cornea, thus, corneal changes may affect iris images.

Small, incremental changes in imaged iris texture over time should be considered normal, as "... age related changes take place in all ocular tissues of the human eye..." [2]. The relevant question for iris biometrics is the time scale at which normal aging has an appreciable effect on the biometric template computed from the imaged iris texture. To underscore this point, we quote from the Flom and Safir iris recognition patent [11]-"The basic, significant features of the iris remain extremely stable and do not change over a period of many years. Even features which do develop over time, such as the

atrophic areas discussed above, usually develop rather slowly, so than an updated iris image will permit identification for a substantial length of time". In this quote, it is clear that Flom and Safir anticipated the possibility that small, incremental changes in iris texture could potentially result in the need for an "updated image" and re-enrollment of the iris template. One interpretation of our results is that they confirm that the possibility that Flom and Safir envisioned is in fact true.

In an attempt to identify the regions of the iris that changed, degrading the match quality, we visually examined the iris images. Visual examination of the iris image pairs with the poorest match scores for the IrisBEE algorithm revealed no drastic or obvious changes in the irises or their textures. This suggests that, if the template aging effect is due to normal aging of the eye, humans may not be able to easily perceive the subtle changes that are involved.

Much additional research remains to be done in the area of template aging for iris biometrics. While

we have experimentally observed a template aging effect, and have ruled out several factors as primary causes of the observed effect, we have not conclusively identified a primary cause of the observed template aging. It is important to understand the cause of the observed template aging effect, so that techniques can be developed to mitigate the effect. It would also be valuable to know whether or not iris biometric template aging is constant across different demographic groups, and whether it occurs at a faster or slower rate as a person ages. Studies that collect new and larger data sets, involve a larger pool of subjects, different sensors, a longer time period, and / or a sample of subjects that represent a greater range of demographics would all be important.

Acknowledgements SEB, KWB, and PJF were supported by the National Science Foundation under grant CNS01-30839, by the Central Intelligence Agency, by the Intelligence Advanced Research Projects Activity and by the Technical Support

Working Group under US Army contract W91CRB-08-C-0093. PJP acknowledges the support of the Biometric Task Force, the Department of Homeland Security's Directorate for Science and Technology, the Intelligence Advanced Research Projects Activity (IARPA), the Federal Bureau of Investigation (FBI), and the Technical Support Working Group (TSWG).

The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of our sponsors. The identification of any commercial product or trade name does not imply endorsement or recommendation by the authors, the University of Notre Dame, or the National Institute of Standards and Technology.

References

1. P. Artal, "Chapter 3: Aging effects on the optics of the eye," in Age-Related Changes of the Human Eye, Carlo A.P. Cavallotti and Lucianon

145

Cerulli, editors, Humanan Press, Totowa, NJ, 2008

2. D. Atchison, E. Markwell, S. Kasthurirangan, J. Pope, G. Smith, P. Swann. "Age-related changes in optical and biometric characteristics of emmetropic eyes," Journal of Vision 8(4):29, 1-20, 2008.

3. S. Baker, A. Hentz, K.W. Bowyer and P.J. Flynn, "Degradation of iris recognition performance due to non-cosmetic prescription contact lenses", Computer Vision and Image Understanding 114 (9), 1030-1044. Sept. 2010.

4. S. Baker, K. Bowyer, P. Flynn, "Empirical Evidence for Correct Iris Match Score Degradation with Increased Time-Lapse Between Gallery and Probe Matches." In Proc. Third International Conference on Biometrics. 1170-1179, 2009.

5. L. Bito, A. Matheny, K. Cruickshanks, D. Nondahl, O. Carino, "Eye color changes past

early childhood," Archives of Ophthalmology, 115, 659-663, May 1997.

6. K.W. Bowyer, K. Hollingsworth, and P. Flynn. "Image Understanding for Iris Biometrics: A Survey." Computer Vision and Image Understanding, 110(2):281-307, 2008.

7. J.W. Carls, R. Raines, M. Grimaila, S. Rogers, "Biometric enhancements: Template aging error score analysis", 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition, 2008. FG '08. Sept 2008, 1-8.

8. J. Daugman, "How Iris Recognition Works," IEEE Transactions On Circuits and Systems for Video Technology, 14(1):21-30, 2004.

9. S. Fenker, K.W. Bowyer, "Experimental evidence of a template aging effect in iris biometrics," IIEEE Computer Society Workshop on Applications of Computer Vision. January 2011.

10. J. Daugman, "New Methods in Iris Recognition," IEEE Transactions On Systems, Man, and Cybernetics. 37(5):1167-1175, Oct 2007.

11. L. Flom, A. Safir, "Iris Recognition Systems," U.S. Patent No. 4641394, 1987.

12. D. Hu, "Photobiology of the Uveal Tract," Photobiological Sciences Online, Kendric C.Smith, editor, http://www.photobiology.info/.

13. K. Hollingsworth, K.W. Bowyer, P.J. Flynn, "Pupil Dilation Degrades Iris Biometric Performance," Computer Vision and Image Understanding, 113(1): Jan 2009.

14. K. Hollingsworth, K.W. Bowyer, P.J. Flynn, "The Best Bits in an Iris Code," IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(6): June 2009.

15. Hollingsworth, K.W. Bowyer, P.J. Flynn, "Similarity of Iris Texture Between Identical

Twins," Computer Vision and Pattern Recognition Biometrics Workshop, June 2010.

16. LG. http://www.lgiris.com/, accessed April 2009.

17. LGE Iris Tech Win In India Redefines Biometric Scalability.http://www.findbiometrics.com/article/115, accessed April 2009

18. N. Kalka, J. Zuo, A. Schmid, B. Cukic, "Image Quality Assessment for Iris Biometrics," In Proc. Biometric Technology for Human Identification III, 6202(1) 2006.

19. A. Lanitis, "A survey of the effects of aging on biometric identity verification", Int'l Journal of Biometrics, 2(1): 34-62 2010.

20. X. Liu, K.W. Bowyer, P. Flynn. "Experiments with an improved iris segmentation algorithm," In Proc. Fourth IEEE Workshop on Automatic Identification Technologies", 118-123, Oct 2005.

21. X. Liu. "Optimizations in Iris Recognition." PhD Dissertation, University of Notre Dame, 2006.

22. K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, H. Nakajima. "An Effective Approach for Iris Recognition Using Phase-Based Image Matching," IEEE Transactions on Pattern Analysis and Machine Intelligence, 30(10):1741-1756, Oct. 2008.

23. The Merck Manual of Geriatrics, 3rd edition, Mark H. Beers, editor, Chapter 126: Aging and the Eye, http://www.merck.com/mkgr/mmg/sec15/ sec15.jsp.

24. D. Monro, S. Rakshit, D. Zhang. "DCT-Based Iris Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4):586-595, April 2007.

25. P. Phillips, W. Scruggs, A. O'Toole, P. Flynn, K. Bowyer, C. Schott, M. Sharpe, "FRVT 2006 and ICE 2006 Large-Scale Experimental Results,"

IEEE Transactions on Pattern Analysis and Machine Intelligence, 32: 831-846, 2010.

26. P.J. Phillips, K. Bowyer, P. Flynn, X. Liu, T. Scruggs "The Iris Challenge Evaluation 2005" In Proc. Second IEEE Conference on Biometrics: Theory, Applications, and Systems. Sept. 2008.

27. P.J. Phillips, P. Grother, R. Michaels, D. Blackburn, E. Tabassi, M. Bone, "Face Recognition Vendor Test 2002: Overview and Summary", 4 March 2000.

28. J. Ryu, J. Jang, H. Kim, "Analysis of Effect of Fingerprint Sample Quality in Template Aging", NIST Biometric Quality Workshop II, Nov 7-8, 2007.

29. P. Tome-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, "On the Effects of Time Variability in Iris Recognition" In Proc. Second IEEE Conference on Biometrics: Theory, Applications and Systems. Sept. 2008.

30. J. Thornton, M. Savvides, V. Kumar. "A Bayesian Approach to Deformed Pattern Matching of Iris Images," IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4):596-606, April 2007.

31. U. Uludag, A. Ross, A. Jain, "Biometric Template Selection and Update: a Case Study in Fingerprints", Pattern Recognition, 37: 1533-1542 2004.

32. VeriEye Iris Recognition Technology. http://www.neurotechnology.com/verieye.html, accessed November 2008.

33. B. Winn, D. Whitaker, D. Elliot, N. Phillips, "Factors Affecting Light-adapted Pupil Size in Normal Human Subjects", Investigative Ophthalmology and Visual Science, 35(3): 1132-1137 1994.

34. K. Wright, P. Spiegel, Pediatric Ophthalmology and Strabismus, Springer-Verlag, New York, 2003, page 438.