THE CENTRE FOR internet & society

Report on Understanding Aadhaar and its New Challenges

Notes from a workshop organised in Delhi on May 26-27, 2016 by the Trans-disciplinary Research Cluster on Sustainability Studies at Jawaharlal Nehru University, Free Software Movement of India, Knowledge Commons, PEACE, Center for Advancement of Public Understanding of Science & Technology, and the Centre for Internet and Society

31st August, 2016

Japreet Grewal, Vanya Rakesh,
Sumandro Chattapadhyay, and Elonnai Hickok

The Trans-disciplinary Research Cluster on Sustainability Studies at Jawaharlal Nehru University ("JNU") collaborated with the Centre for Internet and Society, and other individuals and organisations to organise a two day workshop on "Understanding Aadhaar and its New Challenges" at the Centre for Studies in Science Policy, JNU on May 26 and 27, 2016. The objective of the workshop was to bring together experts from various fields, who have been rigorously following the developments in the Unique Identification Project ("UID Project") and align their perspectives and develop a shared understanding of the status of the UID Project and its impact. Through this exercise, it was also sought to develop a plan of action to address the issues that have arisen by rolling out the UID Project.

This Report is a compilation of the observations made by participants at the workshop relating to myriad issues under the UID Project and various strategies that could be pursued to address these issues.

Acknowledgements

The Centre for Internet and Society is most grateful to all the organisers, speakers, and participants at the workshop for contributing to an extensive and intensive discussion of various aspects of and concerns related to the UID project. We would especially like to express our gratitude to the following for the successful organisation of the workshop: Chinmayi Arun, Dinesh Abrol, S Prasanna, Rajiv Mishra, Reetika Khera, Sanjay Kumar, Sarvjeet Singh, and Usha Ramanathan.

Designed by Saumyaa Naidu

Contents

1. Brief Background of the UID Project

In the year 2009, the UIDAI was established and the UID project was conceived by the Planning Commission under the UPA government to provide unique identification for each resident in India and to be used for delivery of welfare government services in an efficient and transparent manner, along with using it as a tool to monitor government schemes. The objective of the scheme has been to issue a unique identification number by the Unique Identification Authority of India, which can be authenticated and verified online. It was conceptualized and implemented as a platform to facilitate identification and avoid fake identity issues and delivery of government benefits based on the demographic and biometric data available with the Authority.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the "**Act**") was passed as a money bill on March 16, 2016 and was notified in the gazette March 25, 2016 upon receiving the assent of the President. However, the enforceability date has not been mentioned due to which the bill has not come into force.

The Act provides that the Aadhaar number can be used to validate a person's identity, but it cannot be used as a proof of citizenship. Also, the government can make it mandatory for a person to authenticate her/his identity using Aadhaar number before receiving any government subsidy, benefit, or service. At the time of enrolment, the enrolling agency is required to provide notice to the individual regarding how the information will be used, the type of entities the information will be shared with and their right to access their information. Consent of an individual would be obtained for using his/her identity information during enrolment as well as authentication, and would be informed of the nature of information that may be shared. The Act clearly lays that the identity information of a resident shall not be sued for any purpose other than specified at the time of authentication and disclosure of information can be made only pursuant to an order of a court not inferior to that of a District Judge and/or disclosure made in the interest of national security.

2. Legal Status of the UIDAI Project

In this section, we have summarised the discussions on the procedural issues with the passage of the Act. The participants had criticised the passage of the Act as a money bill in the Parliament. The participants also assessed the litigation pending in the Supreme Court of India that would be affected by this law. These discussions took place in the session titled, 'Current Status of Aadhaar' and have been summarised below.

Procedural Issues with Passage of the Act

The participants contested the introduction of the Act in the form of a money bill. The rationale behind this was explained at the session and is briefly explained here. Article 110 (1) of the Constitution of India defines a money bill as one containing provisions only regarding the matters enumerated or any matters incidental to the following: a) imposition, regulation and abolition of any tax, b) borrowing or other financial obligations of the Government of India, c) custody, withdrawal from or payment into the Consolidated Fund of India (CFI) or Contingent Fund of India, d) appropriation of money out of CFI, e) expenditure charged on the CFI or f) receipt or custody or audit of money into CFI or public account of India. The Act makes references to benefits, subsidies and services which are funded by the Consolidated Fund of India (CFI), however the main objectives of the Act is to create a right to obtain a unique identification number and provide for a statutory mechanism to regulate this process. The Act only establishes an identification mechanism which facilitates distribution of benefits and subsidies funded by the CFI and this identification mechanism (Aadhaar number) does not give it the character of a money bill. Further, money bills can be introduced only in the Lok Sabha, and the Rajya Sabha cannot make amendments to such bills passed by the Lok Sabha. The Rajya Sabha can suggest amendments, but it is the Lok

Sabha's choice to accept or reject them. This leaves the Rajya Sabha with no effective role to play in the passage of the bill.

The participants also briefly examined the writ petition that has been filed by former Union minister Jairam Ramesh challenging the constitutionality and legality of the treatment of this Act as a money bill which has raised the question of judiciary's power to review the decisions of the speaker. Article 122 of the Constitution of India provides that this power of judicial review can be exercised to look into procedural irregularities. The question remains whether the Supreme Court will rule that it can determine the constitutionality of the decision made by the speaker relating to the manner in which the Act was introduced in the Lok Sabha. A few participants mentioned that similar circumstances had arisen in the case of Mohd. Saeed Siddiqui v. State of U.P.[1] where the Supreme Court refused to interfere with the decision of the Uttar Pradesh legislative assembly speaker certifying an amendment bill to increase the tenure of the Lokayukta as a money bill, despite the fact that the bill amended the Uttar Pradesh Lokayukta and UP-Lokayuktas Act, 1975, which was passed as an ordinary bill by both houses. The Court in this case held that the decision of the speaker was final and that the proceedings of the legislature being important legislative privilege could not be inquired into by courts. The Court added, "the question whether a bill is a money bill or not can be raised only in the state legislative assembly by a member thereof when the bill is pending in the state legislature and before it becomes an Act."

However, it is necessary to carve a distinction between Rajya Sabha and State Legislature. Unlike the State Legislature, constitution of Rajya Sabha is not optional therefore significance of the two bodies in the parliamentary process cannot be considered the same. Participants also made another significant observation about a similar bill on the UID project (National Identification Authority of India (NIDAI) Bill) that was introduced before by the UPA government in 2010 and was deemed unacceptable by the standing committee on finance, headed by Yashwant Sinha. This bill was subsequently withdrawn.

Status of Related Litigation

A panellist in this session briefly summarised all the litigation that was related to or would be affected by the Act. The panellist also highlighted several Supreme Court orders in the case of *KS Puttuswamy v. Union of India*[2] which limited the use of Aadhaar. We have reproduced the presentation below.

- *KS Puttuswamy v. Union of India* – This petition was filed in 2012 with primary concern about providing Aadhaar numbers to illegal immigrants in India. It was contended that this could not be done without a law establishing the UIDAI and amendment to the Citizenship laws. The petitioner raised concerns about privacy and fallibility of biometrics.
- *Sudhir Vombatkere & Bezwada Wilson*[3] – This petition was filed in 2013 on grounds of infringement of right to privacy guaranteed under Article 21 of the Constitution of India and the security threat on account of data convergence.
- *Aruna Roy & Nikhil Dey*[4] – This petition was filed in 2013 on the grounds of large scale exclusion of people from access to basic welfare services caused by UID. After their petition, no. of intervention applications were filed. These were the following:
- *Col. Mathew Thomas*[5] – This petition was filed on the grounds of threat to national security posed by the UID project particularly in relation to arrangements for data sharing with foreign companies (with links to foreign intelligence agencies).
- *Nagrik Chetna Manch*[6] – This petition was filed in 2013 and led by Dr. Anupam Saraph

[1] Civil Appeal No. 4853 of 2014
[2] WP(C) 494/2012
[3] WP(C) 829/2013
[4] WP(C) 833/2013
[5] WP (C) 37/2015; (Earlier intervened in the Aruna Roy petition in 2013)

on the grounds that the UID project was detrimental to financial service regulation and financial *inclusion*.

- *S. Raju* [7] – This petition was filed on the grounds that the UID project had implications on the federal structure of the State and was detrimental to financial inclusion.
- *Beghar Foundation* – This petition was filed in 2013 in the Delhi High Court on the grounds invasion of privacy and exclusion specifically in relation to the homeless. It subsequently joined the petition filed by Aruna Roy and Nikhil Dey as an intervener.
- *Vickram Crishna* – This petition was originally filed in the Bombay High Court in 2013 on the grounds of surveillance and invasion of privacy. It was later transferred to the Supreme Court.
- *Somasekhar* – This petition was filed on the grounds of procedural unreasonableness of the UID project and also exclusion & privacy. The petitioner later intervened in the petition filed by Aruna Roy and Nikhil Dey in 2013.
- *Rajeev Chandrashekhar* – This petition was filed on the ground of lack of legal sanction for the UID project. He later intervened in the petition filed by Aruna Roy and Nikhil Dey in 2013. His position has changed now.
- Further, a petition was filed by Mr. Jairam Ramesh initially challenging the passage of the Act as a money bill but subsequently, it has been amended to include issues of violation of right to privacy and exclusion of the poor and has advocated for five amendments that were suggested to the Aadhaar Bill by the Rajya Sabha.

Relevant Orders of the Supreme Court

There are six orders of the Supreme Court which are noteworthy.

- **Order of Sept. 23, 2013** - The Supreme court directed that: 1) no person shall suffer for not having an Aadhaar number despite the fact that a circular by an authority makes it mandatory; 2) it should be checked if a person applying for Aadhaar number voluntarily is entitled to it under the law; and 3) precaution should be taken that it is not be issued to illegal immigrants.
- **Order of 26th November, 2013** – Applications were filed by UIDAI, Ministry of Petroleum & Natural Gas, Govt of India, Indian Oil Corporation, BPCL and HPCL for modifying the September 23rd order and sought permission from the Supreme Court to make Aadhaar number mandatory. The Supreme Court held that the order of September 23rd would continue to be effective.
- **Order of 24th March, 2014** – This order was passed by the Supreme Court in a special leave petition filed in the case of UIDAI v CBI [8] wherein UIDAI was asked to UIDAI to share biometric information of all residents of a particular place in Goa to facilitate a criminal investigation involving charges of rape and sexual assault. The Supreme Court restrained UIDAI from transferring any biometric information of an individual without to any other agency without his consent in writing. The Supreme Court also directed all the authorities to modify their forms/circulars/likes so as to not make Aadhaar number mandatory.
- **Order of 16th March, 2015** - The SC took notice of widespread violations of the order passed on September 23rd, 2013 and directed the Centre and the states to adhere to these orders to not make Aadhaar compulsory.

[6] WP (C) 932/2015

[7] Transferred from Madras HC 2013

[8] SLP (Crl) 2524/2014 filed against the order of the Goa Bench of the Bombay HC in CRLWP 10/2014 wherein the High Court had directed UIDAI to share biometric information held by them of all residents of a particular place in Goa to help with a criminal investigation in a case involving charges of rape and sexual assault.

- **Orders of August 11, 2015 –** In the first order, the Central Government was directed to publicise the fact that Aadhaar was voluntary. The Supreme Court further held that provision of benefits due to a citizen of India would not be made conditional upon obtaining an Aadhaar number and restricted the use of Aadhaar to the PDS Scheme and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene and the LPG Distribution Scheme. The Supreme Court also held that information of an individual that was collected in order to issue an Aadhaar number would not be used for any purpose except when directed by the Court for criminal investigations. Separately, the status of fundamental right to privacy was contested and accordingly the Supreme Court directed that the issue be taken up before the Chief Justice of India.
- **Orders of October 16, 2015 –** The Union of India, the states of Gujarat, Maharashtra, Himachal Pradesh and Rajasthan, and authorities including SEBI, TRAI, CBDT, IRDA, RBI applied for a hearing before the Constitution Bench for modification of the order passed by the Supreme Court on August 11 and allow use of Aadhaar number schemes like The Mahatma Gandhi National Rural Employment Guarantee Scheme MGNREGS), National Social Assistance Programme (Old Age Pensions, Widow Pensions, Disability Pensions) Prime Minister's Jan Dhan Yojana (PMJDY) and Employees' Providend Fund Organisation (EPFO). The Bench allowed the use of Aadhaar number for these schemes but stressed upon the need to keep Aadhaar scheme voluntary until the matter was finally decided.

Status of These Orders

The participants discussed the possible impact of the law on the operation of these orders. A participant pointed out that matters in the Supreme Court had not become infructuous because fundamental issues that were being heard in the Supreme Court had not been resolved by the passage of the Act. Several participants believed that the aforementioned orders were effective because the law had not come into force. Therefore, Aadhaar number could only be used for purposes specified by the Supreme Court and it could not be made mandatory. Participants also highlighted that when the Act was implemented, it would not nullify the orders of the Supreme Court unless Union of India asked the Supreme Court for it specifically and the Supreme Court sanctioned that.

3. National Identity Projects in Other Jurisdictions

A panellist had provided a brief overview of similar programs on identification that have been launched in other jurisdictions including Pakistan, United Kingdom, France, Estonia and Argentina in the recent past in the session titled 'Aadhaar - International Dimensions'. This presentation mainly sought to assess the incentives that drove the governments in these jurisdictions to formulate these projects, mandatory nature of their adoption and their popularity. The Report has reproduced the presentation here.

Pakistan

The Second Amendment to the Constitution of Pakistan in 2000 established the National Database and Regulation Authority in the country, which regulates government databases and statistically manages the sensitive registration database of the citizens of Pakistan. It is also responsible for issuing national identity cards to the citizens of Pakistan. Although the card is not legally compulsory for a Pakistani citizen, it is mandatory for:

- Voting
- Obtaining a passport
- Purchasing vehicles and land
- Obtaining a driver licence

- Purchasing a plane or train ticket
- Obtaining a mobile phone SIM card
- Obtaining electricity, gas, and water
- Securing admission to college and other post-graduate institutes
- Conducting major financial transactions

Therefore, it is pretty much necessary for basic civic life in the country. In 2012, NADRA introduced the Smart National Identity Card, an electronic identity card, which implements 36 security features. The following information can be found on the card and subsequently the central database: Legal Name, Gender (male, female, or transgender), Father's name (Husband's name for married females), Identification Mark, Date of Birth, National Identity Card Number, Family Tree ID Number, Current Address, Permanent Address, Date of Issue, Date of Expiry, Signature, Photo, and Fingerprint (Thumbprint). NADRA also records the applicant's religion, but this is not noted on the card itself. (This system has not been removed yet and is still operational in Pakistan.)

United Kingdom

The Identity Cards Act was introduced in the wake of the terrorist attacks on 11th September, 2001, amidst rising concerns about identity theft and the misuse of public services. The card was to be used to obtain social security services, but the ability to properly identify a person to their true identity was central to the proposal, with wider implications for prevention of crime and terrorism. The cards were linked to a central database (the National Identity Register), which would store information about all of the holders of the cards. The concerns raised by human rights lawyers, activists, security professionals and IT experts, as well as politicians were not to do with the cards as much as with the NIR. The Act specified 50 categories of information that the NIR could hold, including up to 10 fingerprints, digitised facial scan and iris scan, current and past UK and overseas places of residence of all residents of the UK throughout their lives. The central database was purported to be a prime target for cyber attacks, and was also said to be a violation of the right to privacy of UK citizens. The Act was passed by the Labour Government in 2006, and repealed by the Conservative-Liberal Democrat Coalition Government as part of their measures to "reverse the substantial erosion of civil liberties under the Labour Government and roll back state intrusion."

Estonia

The Estonian i-card is a smart card issued to Estonian citizens by the Police and Border Guard Board. All Estonian citizens and permanent residents are legally obliged to possess this card from the age of 15. The card stores data such as the user's full name, gender, national identification number, and cryptographic keys and public key certificates. The cryptographic signature in the card is legally equivalent to a manual signature, since 15 December 2000. The following are a few examples of what the card is used for:

- As a national ID card for legal travel within the EU for Estonian citizens
- As the national health insurance card
- As proof of identification when logging into bank accounts from a home computer
- For digital signatures
- For i-voting
- For accessing government databases to check one's medical records, file taxes, etc.
- For picking up e-Prescriptions
- (This system is also operational in the country and has not been removed)

France

The biometric ID card was to include a compulsory chip containing personal information, such as fingerprints, a photograph, home address, height, and eye colour. A second, optional chip was to be implemented for online authentication and electronic signatures, to be used for e-government services and e-commerce. The law was passed with the purpose of combating " identity fraud". It was referred to the Constitutional Council by more than 200 members of the French Parliament, who challenged the compatibility of the bill with the citizens' fundamental rights, including the right to privacy and the presumption of innocence. The Council struck down the law, citing the issue of proportionality. "Regarding the nature of the recorded data, the range of the treatment, the technical characteristics and conditions of the consultation, the provisions of article 5 touch the right to privacy in a way that cannot be considered as proportional to the meant purpose".

Argentina

Documento Nacional de Identidad or DNI (which means National Identity Document) is the main identity document for Argentine citizens, as well as temporary or permanent resident aliens. It is issued at a person's birth, and updated at 8 and 14 years of age simultaneously in one format: a card (DNI tarjeta); it's valid if identification is required, and is required for voting. The front side of the card states the name, sex, nationality, specimen issue, date of birth, date of issue, date of expiry, and transaction number along with the DNI number and portrait and signature of the card's bearer. The back side of the card shows the address of the card's bearer along with their right thumb fingerprint. The front side of the DNI also shows a barcode while the back shows machine-readable information. The DNI is a valid travel document for entering Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay, and Venezuela. (System still operational in the country)

4. Technologies of Identification and Authentication

The panel in the session titled 'Aadhaar: Science, Technology, and Security' explained the technical aspects of use of biometrics and privacy concerns, technology architecture for identification and inadequacy of infrastructure for information security. In this section, we have summarised the presentation and the ensuing discussions on these issues.

Use of Biometric Information for Identification and Authentication

The panellist explained with examples that identification and authentication were different things. Identity provides an answer to the question "who are you?" while authentication is a challenge-response process that provides a proof of the claim of identity. Common examples of identity are User ID (Login ID), cryptographic public keys and ATM or Smart cards while common authenticators are passwords (including OTPs), PINs and cryptographic private keys. Identity is public information but an authenticator must be private and known only to the user. Authentication must necessarily be a conscious process and active participation by the user is a must. It should also always be possible to revoke an authenticator. After providing this understanding of the two processes the panellist then explained if biometric information could be used for identification or authentication under the UID Project. Biometric information is clearly public information and it is questionable if it can be revoked. Therefore it should never be used for authentication, but only for identity verification. There is a possibility of authentication by fingerprints under the UID Project, without conscious participation of the user. One could trace the fingerprints of an individual from any place the individual has been in contact with. Therefore, authentication must certainly be done by other means. The panellist pointed out that there were five kinds of authentication under the UID Project, out of which two-factor authentication and one time password were considered suitable but use of biometric information and demographic information was extremely threatening and must be withdrawn.

Architectures of Identification

The panellist explained the architecture of the UID Project that has been designed for identification purposes, highlighted its limitations and suggested alternatives. His explanations are reproduced below.

Under the UID Project, there is a centralised means of identification i.e. the Aadhaar number and biometric information stored in one place, Central Identification Data Repository (CIDR). It is better to have multiple means of identification than one (as contemplated under the UID Project) for preservation of our civil liberties. The question is what the available alternatives are. Web of trust is a way for operationalizing distributed identification but the challenge is how one brings people from all social levels to participate in it. There is a need for registrars who will sign keys and public databases for this purpose.

The Aadhaar number functions as a common index and facilitates correlation of data across Government databases. While this is tremendously attractive it raises several privacy concerns as more and more information relating to an individual is available to others and is likely to be abused.

The Aadhaar number is available in human readable form. This raises the risk of identification without consent and unauthorised profiling. It cannot be revoked. Potential for damage in case of identity theft increases manifold.

Under the UID Project, for the purpose of information security, Authentication User Agencies (“**AUA**”) are required to use local identifiers instead of Aadhaar numbers but they are also required to map these local identifiers to the Aadhaar numbers. Aadhaar numbers are not cryptographically secured; in fact they are publicly available. Hence this exercise for securing information is useless. An alternative would be to issue different identifiers for different domains and cryptographically embed a “master identifier” (in this case, equivalent of Aadhaar number) into each local identifier.

All field devices (for example POS machines) should be registered and must communicate directly with UIDAI. In fact, UIDAI must verify the authenticity (tamper proof) of the field device during run time and a UIDAI approved authenticity certificate must be issued for field devices. This certificate must be made available to users on demand. Further, the security and privacy frameworks within which AUAs work must be appropriately defined by legal and technical means.

Security Infrastructure of CIDR

The panellists also enumerated the security features of the UID Project and highlighted the flaws in these features. These have been summarised below.

The security and privacy infrastructure of UIDAI has the following main features:

- 2048 bit PKI encryption of biometric data in transit
- End-to-end encryption from enrolment/POS to CIDR
- HMAC based tamper detection of PID blocks
- Registration and authentication of AUAs
- Within CIDR only a SHA 1 Hash of Aadhaar number is stored
- Audit trails are stored SHA 1 encrypted. Tamper detection?
- Only hashes of passwords and PINs are stored. (biometric data stored in original form though!)
- Authentication requests have unique session keys and HMAC
- Resident data stored using 100 way sharding (vertical partitioning). First two digits of Aadhaar number as shared keys

- All enrolment and update requests link to partitioned databases using Ref IDs (coded indices)
- All accesses through a hardware security module
- All analytics carried out on anonymised data

The panellists pointed out the concerns about information security on account of design flaws, lack of procedural safeguards, openness of the system and too much trust imposed on multiple players. All symmetric and private keys and hashes are stored somewhere within UIDAI. This indicates that trust is implicitly assumed which is a glaring design flaw. There is no well-defined approval procedure for data inspection, whether it is for the purpose of investigation or for data analytics. There is a likelihood of system hacks, insider leaks, and tampering of authentication records and audit trails. The ensuing discussions highlighted that the UIDAI had admitted to these security risks. The enrolment agencies and the enrolment devices cannot be trusted. AUAs cannot be trusted with biometric and demographic data; neither can they be trusted with sensitive user data of private nature. There is a need for an independent third party auditor for distributed key management, auditing and approving UIDAI programs, including those for data inspection and analytics, whitebox cryptographic compilation of critical parts of the UIDAI programs, issue of cryptographic keys to UIDAI programs for functional encryption, challenge-response for run-time authentication and certification of UIDAI programs. The panellist recommended that there was a need to put a suitable legal framework to execute this.

The participants also discussed that information infrastructure must not be made of proprietary software (possibility for backdoors for US) and there must be a third party audit with a non-negotiable clause for public audit.

5. Aadhaar for Welfare?

The Report has summarised the discussions that took place in the sessions on ‘Direct Benefits Transfers’ and ‘Aadhaar: Broad Issues - II’ where the panellists critically analysed the claims of benefits and inclusion of Aadhaar made by the government in light of the ground realities in states where Aadhaar has been adopted for social welfare schemes.

Social Welfare: Modes of Access and Exclusion

Under the Act, a person may be required to authenticate or give proof of the Aadhaar number in order to receive subsidy from the government (Section 7). A person is required to punch their fingerprints on POS machines in order to receive their entitlement under the social welfare schemes such as LPG and PDS. It was pointed out in the discussions that various states including Rajasthan and Delhi had witnessed fingerprint errors while doling out benefits at ration shops under the PDS scheme. People have failed to receive their entitled benefits because of these fingerprint errors thus resulting in exclusion of beneficiaries.[9] A panellist pointed out that in Rajasthan, dysfunctional biometrics had led to further corruption in ration shops. Ration shop owners often lied to the beneficiaries about functioning of the biometric machines (POS Machines) and kept the ration for sale in the market therefore making a lot of money at the expense of uninformed beneficiaries and depriving them of their entitlements.

Another participant organisation also pointed out similar circumstances in the ration shops in Patparganj and New Delhi constituencies. Here, the dealers had maintained the records of beneficiaries who had been categorized as follows: beneficiaries whose

[9] See: http://scroll.in/article/806243/rajasthan-presses-on-with-aadhaar-after-fingerprint-readers-fail-well-buy-iris-scanners

biometrics did not match, beneficiaries whose biometrics matched and entitlements were provided, beneficiaries who never visited the ration shop. It had been observed that there were no entries in the category of beneficiaries whose biometrics did not match however, the beneficiaries had a different story to tell. They complained that their biometrics did not match despite trying several times and there was no mechanism for a manual override. Consequently, they had not been able to receive any entitlements for months. The discussions also pointed out that the food authorities had placed complete reliance on authenticity of the POS machines and claim that this system would weed out families who were not entitled to the benefits. The MIS was also running technical glitches as a result there was a problem with registering information about these transactions hence, no records had been created with the State authority about these problems. A participant also discussed the plight of 30,000 widows in Delhi, who were entitled to pension and used to collect their entitlement from post offices, faced exclusion due to transition problems under the Jan Dhan Yojana (after the Jandhan was launched the money was transferred to their bank accounts in order to resolve the problem of misappropriation of money at the hands of post office officials). These widows were asked to open bank accounts to receive their entitlements and those who did not open these accounts and did not inform the post office were considered bogus.

In the discussions, the participants also noted that this unreliability of fingerprints as a means of authentication of an individual's identity was highlighted at the meeting of Empowered Group of Ministers in 2011 by J Dsouza, a biometrics scientist. He used his wife's fingerprints to demonstrate that fingerprints may change overtime and in such an event, one would not be able to use the POS machine anymore as the machine would continue to identify the impressions collected initially.

The participants who had been working in the field had contributed to the discussions by busting the myth that the UID Project helped to identify who was poor and resolve the problem of exclusion due to leakages in the social welfare programs. These discussions have been summarised below.

- It is important to understand that the UID Project is merely an identification and authentication system. It only helps in verifying if an individual is entitled to benefits under a social security scheme. It does not ensure plugging of leakages and reducing corruption in social security schemes as has been claimed by the Government. The reduction in leakage of PDS, for instance, should be attributed to digitization and not UID. The Government claims, that it has saved INR 15000 crore in provision of LPG on identification of 3.34 crore inactive accounts on account of the UID Project. This is untrue because the accounts were weeded by using mechanisms completely unrelated to the UID Project. Consequently, the savings on account of UID are only of INR 120 crore and not 15000 crore.

- The UID Project has resulted in exclusion of people either because they do not have an Aadhaar number, or they have a wrong identification, or there are errors of classification or wilful misclassification. About 99.7% people who were given Aadhaar numbers already had an identification document. In fact, during enrolment a person is required to produce one of 14 identification documents listed under the law in order to get an Aadhaar number which makes it very difficult for a person with no identity to become entitled to a social welfare scheme.

A participant condemned the Government's claim that the UID Project had helped in removing fake, bogus and duplicate cards and said that these terms could not be used synonymously and the authorities had no clarity about the difference between the meanings of these terms. The UID Project had only helped in removal of duplicate cards but had not helped in combating the use of fake and bogus cards.

Financial Inclusion and Direct Benefits Transfer

The participants also engaged in the discussions about the impact of the UID project on financial inclusion in India in the sessions titled 'Aadhaar: Broad Issues - I & II'. We have summarised these discussions below.

The UID Project seeks to directly transfer money to a bank account in order to combat corruption. The discussions highlighted that this was nothing but introducing a neo liberal thrust in social policy and that it was not feasible for various reasons. First, 95% of rural India did not have functioning banks and banks are quite far away. Second, in order to combat this dearth of banks the idea of business correspondents, who handled banking transactions and helped in opening of bank accounts, had been introduced which had created various problems. The Reserve Bank of India reported that there was dearth of business correspondents as there was very little incentive to become one; their salary is merely INR 4000. Third, there were concerns about how an Aadhaar number was considered a valid document for Know Your Customer (KYC) checks. There was a requirement for scrutiny and auditing of documents submitted during the time of enrolment which, in the present scheme of things, could not be verified. Fourth, there were no restrictions on number of bank accounts that could be opened with a single Aadhaar number which gave rise to a possibility of opening multiple and shell accounts on a single Aadhaar number. Therefore, records only showed transactions when money was transferred from an Aadhaar number to another Aadhaar number as opposed to an account-to-account transfer. The discussion relied on NPCI data which shows which bank an Aadhaar number is associated with but does not show if a transaction by an Aadhaar number is overwritten by another bank account belonging to the same Aadhaar number.

6. Surveillance and UIDAI

The participants had discussed the possibility of an alternative purpose for enrolling Aadhaar in the session titled 'Privacy, Surveillance, and Ethical Dimensions of Aadhaar'. The discussion traced the history of this project to gain insight on this issue. We have summarised below the key take aways from this discussion.

There are claims that the main objective of launching the UID Project is not to facilitate implementation of social security schemes but to collect personal (financial and non-financial) information of the citizens and residents of the country to build a data monopoly. For this purpose, PDS was chosen as a suitable social security scheme as it has the largest coverage. Several participants suggested that numerous reports authored by FICCI, KPMG and ASSOCHAM contained proposals for establishing a national identity authority which threw some light on the commercial intentions behind information collection under the UID Project.

It was also pointed out that there was documented proof that information collected under the UID Project might have been shared with foreign companies. There are suggestions about links established between proponents of the UID Project and companies backed by CIA or the French Government which run security projects and deal in data sharing in several jurisdictions.

7. Strategies for Future Action

The participants laid down a list of measures that must be taken to take the discussions forward. We have enumerated these recommendations below.

- Prepare and compile an anthology of articles as an output of this workshop.
- Prepare position papers on specific issues related to the UID Project
- Prepare pamphlets/brochures on issues with the UID Project for public consumption

- Prepare counter-advertisements for Aadhaar
- Publish existing empirical evidence on the flaws in Aadhaar.
- Set up an online portal dedicated to providing updates on the UID Project and allows discussions on specific issues related to Aadhaar.
- Use Social Media to reach out to the public. Regularly track and comment on social media pages of relevant departments of the government.
- Create groups dedicated to research and advocacy of specific aspects of the UID Project.
- Create a Coordination Committee preferably based in Delhi which would be responsible for regularly holding meetings and for preparing a coordinated plan of action. Employ permanent to staff to run the Committee.
- Organise an advocacy campaign against use of Aadhaar in collaboration with other organisations and build public domain acceptance.
- The campaign must specifically focus on the unfettered scope of UID and expanse, misrepresentation of the success of Aadhaar by highlighting real savings, technological flaws, status of pilot programs and increasing corruption on account of the UID Project
- Prepare a statement of public concern regarding the UID Project and collect signatures from eminent persons including academics, technical experts, civil society groups and members of parliament.
- Organise events and discussions on issues relating to Aadhaar and invite members of government departments to speak and discuss the issues.
- Write to Members of Parliament and Members of Legislative Assemblies raising questions on their or their parties’ support for Aadhaar and silence on the problems created by the UID Project.
- Organise public hearings in states like Rajasthan to observe and document ground realities of the UID Project and share these outcomes with the state government and media.
- Plan a national social audit and public hearing on the working of UID Project in the country.
- File Contempt Petitions in the Supreme Court and High Courts against mandatory use of Aadhaar number for services not allowed by the Supreme Court.
- Reach out to and engage with various foreign citizens and organisations that have been fighting on similar issues. The organisations and individuals who could be approached would include EPIC, Electronic Frontier foundation, David Moss, UK, Roger Clarke, Australia, Prof. Ian Angel, Snowden, Assange and Chomsky.
- Work towards increasing awareness about the UID Project and gaining support from the student and research community, student organisations, trade unions, and other associations and networks in the unorganised sector.

Annexure A – Workshop Agenda

May 26, 2016

9:00-9:30	**Registration**
9:30-10:00	Prof. Dinesh Abrol - Welcome
	Self-introduction and expectations of participants
	Dr. Usha Ramanathan - Overview of the Workshop
10:00-11:00	**Current Status of Aadhaar**
	Dr. Usha Ramanathan, Legal Researcher, New Delhi - What the 2016 Law Says, and How it Came into Being
	S. Prasanna, Advocate, New Delhi - Status and Force of Supreme Court Orders on Aadhaar
	Discussion + Q & A
11:00-11:30	**Tea Break**
11:30-13:00	**Direct Benefits Transfers**
	Prof. Reetika Khera, Indian Institute of Technology, Delhi - Welfare Needs Aadhaar like a Fish Needs a Bicycle
	Prof. Ram Kumar, Tata Institute of Social Sciences, Mumbai - Aadhaar and the Social Sector: A critical analysis of the claims of benefits and inclusion
	Ashok Rao, Delhi Science Forum - Cash Transfers Study
	Discussion + Q & A
13:00-13:30	**Video Presentation/s**
13:30-14:30	**Lunch**
14:30-16:00	**Aadhaar: Science, Technology, and Security**
	Prof. Subashis Banerjee, Deptt of Computer Science & Engineering, IIT, Delhi - Privacy and Security Issues Related to the Aadhaar Act
	Pukhraj Singh, former National Cyber Security Manager, Aadhaar, New Delhi - Aadhaar: Security and Surveillance Dimensions
	Discussion + Q & A
16:00-16:30	**Tea Break**
16:30-17:30	**Aadhaar - International Dimensions**
	Prof. Chinmayi Arun, Center for Communication Governance, National Law University, Delhi - Biometrics and Mandatory IDs in other parts of the world
	Dr. Gopal Krishna, Citizens Forum for Civil Liberties - International Dimensions of Aadhaar
17:30-18:00	**High Tea**
18:00-19:00	**Video Presentations**

May 27, 2016

9:30	**Session begins**
9:30-11:00	**Privacy, Surveillance & Ethical Dimensions of Aadhaar**
	Prabir Purkayastha, Free Software Movement of India, New Delhi - Surveillance Capitalism and the Commodification of Personal Data
	Arjun Jayakumar, SFLC - Surveillance Projects Amalgamated
	Col Mathew Thomas, Bengaluru - The Deceit of Aadhaar
11:00-11:30	**Tea Break**
11:30-13:00	**Aadhaar - Broad Issues - I**
	Prof. G Nagarjuna, Homi Bhabha Center for Science Education, Tata Institute of Fundamental Research, Mumbai - How to prevent linked data in the context of Aadhaar
	Dr. Anupam Saraph, Pune - Aadhaar and Moneylaundering
13:00-13:30	Video Screenings
13:30-14:30	**Lunch**
14:30-15:30	**Aadhaar - Broad Issues - II**
	Prof. MS Sriram, Visiting Faculty, Indian Institute of Management, Bangalore - Financial lnclusion
	Nikhil Dey, MKSS, Rajasthan (TBC) - Field witness: Technology on the Ground
	Prof. Himanshu, Centre for Economic Studies & Planning, JNU - UID Process and Financial Inclusion
15:30-16:00	**Conclusion**
16:00-18:00	**Informal Meetings**

Annexure B – Workshop Participants

Dr. Anupam Saraph

Arjun Jayakumar, Software Freedom Law Centre

Ashok Rao, Delhi Science Forum

Prof. Chinmayi Arun, National Law University, Delhi

Prof. Dinesh Abrol, Jawaharlal Nehru University

Prof. G Nagarjuna, Homi Bhabha Center for Science Education,
Tata Institute of Fundamental Research, Mumbai

Dr. Gopal Krishna, Citizens Forum for Civil Liberties

Prof. Himanshu, Jawaharlal Nehru University

Japreet Grewal, the Centre for Internet and Society

Joshita Pai, National Law University, Delhi

Malini Chakravarty, Centre for Budget and Governance Accountability

Col. Mathew Thomas

Prof. MS Sriram, Indian Institute of Management, Bangalore

Nikhil Dey, Mazdoor Kisan Shakti Sangathan

Prabir Purkayastha, Knowledge Commons and Free Software Movement of India

Pukhraj Singh, Bhujang

Rajiv Mishra, Jawaharlal Nehru University

Prof. Ram Kumar, Tata Institute of Social Sciences, Mumbai

Reetika Khera, Indian Institute of Technology, Delhi

Ritajyoti Bandyopadhyay, Indian Institute of Science Education and Research, Mohali

S. Prasanna, Advocate

Sanjay Kumar, Science Journalist

Sharath, Software Freedom Law Centre

Shivangi Narayan, Jawaharlal Nehru University

Prof. Subhashis Banerjee, Indian Institute of Technology, Delhi

Sumandro Chattapadhyay, the Centre for Internet and Society

Dr. Usha Ramanathan, Legal Researcher

Note: This list is only indicative, and not exhaustive.

About the Authors

Japreet Grewal

Japreet works on issues surrounding technology and regulation with emphasis on issues affecting freedom of expression and intermediary liability at the domestic and international levels under the Internet Governance and Freedom of Expression Project at CIS.

Vanya Rakesh

Vanya works as a Programme Officer on Big Data implications in the Global South and Privacy with the Information Policy team at CIS.

Sumandro Chattapadhyay

Sumandro is Research Director at CIS. His academic interests span over topics of history and politics of informatics, new media and technology studies, and data infrastructures and economies. He is also keenly interested in computational techniques in arts, humanities, and social research, and emerging methodological questions.

Elonnai Hickok

Elonnai is Director - Internet Governance at the Centre for Internet and Society, Bangalore. She leads the privacy, surveillance, and big data work at the Centre and has also written extensively on issues pertaining to intermediary liability, digital rights, identity, cyber security and DNA profiling.

About CIS

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and practices around internet, technology and society in India, and elsewhere.

cis-india.org | @cis_india