Date: 15th November, 2017

To,

Chairperson and Members,
Parliamentary Standing Committee on Home Affairs

Sub: Urgent memorandum on privacy and security concerns related to the Aadhaar establishment

In a historic judgment delivered by a 9 judge constitution bench of the Supreme Court on August 24, 2017, Right to Privacy was upheld as a fundamental right, as it was acknowledged as an inalienable right which was an integral aspect of right to life and personal liberty.

It is heartening to note that the Parliamentary Standing Committee on Home Affairs has rightly ascertained the far reaching implications of this ruling on the Aadhaar establishment. News reports of Home Affairs Ministry and UIDAI officials answering pointed questions from the Committee are indeed very encouraging.

The government seems to be downplaying the impact of this ruling by saying that the challenge to Aadhaar is pending before the Supreme Court. Before the Supreme Court, the government is averting any concrete solution by referring to the constitution of Srikrishna Committee. Meanwhile, citizens are being coerced, threatened, inconvenienced in the overzealous drive to link everything with Aadhaar without adequate safeguards in place.

To aid the Committee in its work, we present a summary of the most pertinent privacy and larger security concerns that arise out of the Aadhaar establishment:–

**Privacy related concerns of Aadhaar**

- **Profiling and surveillance** - Aadhaar was never intended as an ubiquitous identity verification mechanism. As opposed to other IDs currently in place used for limited purposes, Aadhaar which stores our biometric information is being ‘seeded’ with a whole range of services - birth certificates, university degrees, PAN cards, SIM cards, insurance records, health records - making it very easy to do ‘profiling’ of an
individual without the consent of the individual. Such profiling can be used for illegal surveillance.

- **Data monetization** - UIDAI allows private companies to use Aadhaar for authentication purposes - like at the time of buying a SIM card. Such private companies use the information associated with Aadhaar (except the biometrics) for commercial purposes, for instance to decide what service to be targeted to which customer - against the consent of the customer. Right now anyone can create their own database of Aadhaar numbers and can further sell such a database also.

- **Insufficient data protection mechanism** - Seeding Aadhaar with all manners of services necessitates a strong and robust data protection regime, in the absence of which, threatening citizens with disruption of services or coercing them to sign up for Aadhaar, is a blatant violation of their privacy right. Privacy is also affected when government looks to collect excessive amounts of data than what is possibly needed, which then runs the risk of leakage or being exploited for commercial purposes.

- **Expansion in usage without consent** - Even when the data was originally captured for a limited range of services, there were widespread concerns about lack of informed and effective consent from the citizens. And now, the use of this sensitive data has been expanded to a wide range of services without consent of the people involved and without any backing of the law - merely through executive orders. In the absence of a law and fresh consent every time, such expansion in usage is violative of right to privacy and directly attacks right to liberty as well as people are being devoid of a choice.

### Security related concerns of Aadhaar

- **Storage in central repository** - The Aadhaar act provides that biometric data is stored in a central repository which also keeps a log of all those instances in which authentication was sought. Such a central repository - which stores valuable personal data about an individual, is not beyond breach, as several instances of data breach has shown.

- **Financial vulnerabilities** - Aadhaar enabled payment systems - seeding Aadhaar number with bank accounts - if finger-print is forged, it can easily lead to banking frauds. In an incident in an engineering college in Mumbai, it was found that close to 200 students used a chemical substance to forge fingerprints and tricked the biometric attendance system. A recent incident also revealed how linking of Aadhaar with bank accounts and SIM could enable criminals to easily perpetrate frauds.

- **Authentication frauds** - In the several instances of data breach which have been shared later, it is seen that just the availability of someone’s Aadhaar number could
lead to possible frauds because one form of authentication is to match Aadhaar number with demographic details. But more importantly, the vulnerability associated with biometrics as a form of authentication has recently come out in the open.

- **Inadequate remedy** - The Aadhaar act provides that if there is data breach, UIDAI gets notification and not the individual whose data it is. Again, it is not the individual whose data has been leaked, but the UIDAI, which can complain against any such breach. If UIDAI doesn’t institute a complaint, individual is left without a remedy. It has been argued that more the number of users of a database, larger the possibilities of its breach, but with no remedy.

**Instances of data breach and other violations**

- In February, 2017, UIDAI filed a police complaint against Axis Bank Pvt. Ltd., and other associated organizations as they stored the biometric data given to them for authentication and then used it to undertake fake transactions without authorization - one individual had reportedly undertaken 397 biometric transactions.
- So far 34,000 agents involved in enrolling have been suspended, fined or blacklisted for various violations, which also included violations related to updating of information in the Aadhaar database.
- As stated by Ajay Bhushan Pandey, CEO of UIDAI - if someone has your Aadhaar number, it is possible to create your 360 degree profile. This is because large amounts of demographic datasets are also associated with Aadhaar number. Despite this, there have been many instances of websites, sometimes government department websites, publicly displaying Aadhaar card details of beneficiaries:-
  1. In February, a website revealed Aadhaar demographic data of over 5 lakh minors
  2. Rural Development Ministry’s website showed Aadhaar card details of 10 crore MNREGA workers.
  3. In April, 2017, website of Food and Civil supplies department of Chandigarh displayed Aadhaar numbers of close to 4.9 lakh PDS beneficiaries
  5. In July 2017, a website displayed phone numbers, addresses and Aadhaar numbers of some Reliance Jio subscribers.
  6. In August 2017, Wikileaks released a report as per which it was alleged that CIA may already be snooping in to Aadhaar database.
  7. In September 2017, a gang of hackers was busted in UP and it was revealed that they had managed to clone the fingerprints of operators and hacked into the Aadhaar
system which allowed them to run fake enrolment agencies by charging Rs.5000/- from each person who gained access. After the system detected a forced entry, it started asking for iris authentication as well and the hackers managed to manipulate the system there also.

8. In September 2017, a girl allegedly died of starvation in Jharkhand after her family stopped receiving rations for several months because their PDS card was not seeded with Aadhaar. Since then, more such deaths in Jharkhand have been reported.

9. In October 2017, a man lost more than a lakh rupees from his salary account in ICICI after his SIM was cloned to hack into his account. He was threatened that if he did not share his SIM details to link it with Aadhaar, his number will be deactivated.

**International perspective - a similar project in United Kingdom shelved in 2010**

- UK had announced a plan to issue National ID cards - a unique number linked to biometric information, with several different categories of data related to an individual in a central National register. It would also include information on every time the card was used.
- In face of massive privacy concerns and immense possibilities of surveillance, the project was ultimately abandoned.

**Pertinent questions to be raised for the Home Ministry officials and UIDAI officials**

- How many instances of breach / attempt to breach of Aadhaar database have been notified to UIDAI and what has been the action taken by UIDAI in all such cases? Especially with respect to the UP incident, it emerged that such gangs may be operating in other states also. If that is so, when did UIDAI detect the UP fraud or fraud going on in any other state and whether it happened while the Supreme Court was hearing the arguments on Privacy. If it did, why were these incidents not brought before the Court?
- Without amending the Aadhaar Act, could the usage of Aadhaar be expanded through notifications and executive orders? Whether people have been given the option of giving or denying their consent every time Aadhaar is sought to be seeded to a new service?
- What is the need for storing and archiving instances of every use of the Aadhaar number when such a database is vulnerable to breach?
- Why have private companies been allowed to require Aadhaar authentication when the initial purpose was to better target government welfare benefits?
• Whether any rules have been put in place to prevent private companies from creating their own databases of Aadhaar and other related information of customers or to sell / share such information to any entity?
• What action was taken against government departments which publicly displayed Aadhaar and other related demographic information about beneficiaries? If no action was taken, why not? [We would also like to highlight that to ensure that transparency is not undermined in the name of privacy, data, other than sensitive Aadhaar data, must still continue to be made available]
• How will the Home Ministry ensure that the entire procedure - right from collecting biometric to its storage to its authentication - is safe from any breach / attack which is likely to raise national security concerns?

The Committee is also requested to undertake a larger stakeholder consultation on this subject and invite evidence and comments from experts, professionals and general public to ascertain the various privacy and security concerns related to Aadhaar. A widespread consultation is likely to generate valuable inputs for the government to act on.

We hope that the arguments and information presented in this memorandum aid you in your extremely important role of keeping a check on government policies and decisions, and ensuring security of citizens and their private data.

To offer further assistance, several experts associated with us, working on Aadhaar related issues, can present their views and concerns before the Committee. Please do not hesitate to reach out in case you require to deliberate on us with the issues mentioned in this memorandum in greater detail or require any further information.

Thank You,
Warm Regards from the Rethink Aadhaar Campaign,

Raghuram S. Godavarthi
Praavita Kashyap
+91-9868869900