IN THE HON'BLE SUPREME COURT OF INDIA

WP (C) NO. 966/2017

IN THE MATTER OF:

RAGHAV TANKHA	...	PETITIONER
Versus		
UNION OF INDIA AND ORS.	...	RESPONDENTS

PROPOSITIONS BY MR. KAPIL SIBAL, SENIOR ADVOCATE – TECHNICAL EVALUATION OF AADHAAR

1. EVALUATION OF CENTRALIZED BIOMETRICS FROM A TECHNICAL STANDPOINT

1.1. **Centralization:** From a security perspective, the Central ID Repository (CIDR) holds out its database to be secure as it is 'federated' i.e. the database is broken up and stored across multiple locations. However, regardless of its physical separation, the entire data in all the locations forms a logic unit because the de-duplication algorithm traverses the full database i.e. the database is digitally connected so that the algorithm used to search the Aadhaar database to see if a person giving her biometrics for issuance of a fresh Aadhaar already exists in the Aadhaar database, can search the entire Aadhaar database at one go. A recent RBI report has identified the CIDR as a "single target" for internal/external/indigenous/foreign attacks and also a "single point of failure". The Report states that "*Thanks to Aadhaar, for the first time in the history of India, there is now a readily available single target for cyber criminals as well as India's external enemies. In a few years, attacking UIDAI data can potentially cripple Indian businesses and administration in ways that were inconceivable a few years ago. The loss to the economy and citizens in case of such an attack is bound to be incalculable.*"[1]

1.2. **Opaque Foreign Technologies:** Even though biometric technologies are based on open standards, the implementations of these standards for the "de-duplication service" and the "authentication service" are proprietary software owned by L-1 Identity Solutions and Morpho S.A.S. This software cannot be independently audited because it is covered by intellectual property law. The employees of L-1 Identity Solutions and Morpho S.A.S, who are employees of

[1] Dr. A.S. Ananth, "Biometrics and its Impact in India", IDBRT Staff Paper Series, Vol. 3, No. 1, October 2017, p. 119.

private foreign entities, have access to the UIDAI's CIDR. As per the contracts between these companies and UIDAI, these foreign companies were given access to all the biometric templates of those persons who were enrolled. There is no way of verifying if these companies have actually deleted these templates after processing.

1.3. **Cost of compromise:** Unlike smart-cards which require several pieces of sophisticated equipment such as a card skimmer and card printer in addition to sophisticated software and advanced technical knowledge to compromise them, most biometric readers in India today can be defeated by a child with no technical knowledge using Fevicol and wax.

1.4. **Cost of recovery from compromise:** Once the national biometric database has been compromised there is nothing we can do to re-secure it. With smart card technology there is no centralized database of secret information which can be permanently compromised. Even if the identifiers are compromised they can be easily reissued. There are already several reported instances of theft of biometric data from various locations.

1.5. **Any leakage or theft of data damages the credibility of the entire system**: It has to be remembered that any leakage of biometric data is permanent. Since this is a means of authentication, to be effective at any point, the entire system must meet the underlying assumption of being 100% accurate. If a few lakh people's biometric data is at large and there is no track of who's data has been stolen, it introduces a doubt into every authentication carried out using the UIDAI. So after a security breach, for every authentication carried out using Aadhaar, the transaction can be challenged on the basis that the data of the individual in question may have been part of the biometric data that was leaked or stolen.

1.6. **Leakage or theft of biometric data and its impact on criminal investigation**: Leakage or theft of biometric data infusesreasonable doubt into every criminal trial where fingerprints lifted from the crime scene are sought to be used as evidence. Since fingerprints can be recreated using a scan, once a portion of biometric data is at large, there is no way of saying with certainty that the fingerprints of the accused being found at the crime scene prove beyond reasonable doubt that the accused actually visited the crime scene.

1.7. **Man in the Middle Attacks:** Since an individual's biometric data is just an electronic file, 'Man in the Middle Attacks' attacks are possible by four entities during the usage of biometrics on phones - Operating System Vendor [for ex. Google and Apple], Hardware Vendor [for ex. Samsung and Lenovo], Telecommunication company [for ex. Airtel and Reliance] and Internet Service Provider [for ex. Spectranet and Asianet]. Similarly, during usage of biometrics on POS machines (such as those used at Banks, PDS shops etc) and enrollment machines, an additional route of attack is by the use of a USB connector cable attached between the biometric reader and the computer. The fact that these attacks are possible has been implicitly acknowledged by UIDAI because the UIDAI has tried to address these potential compromises by releasing proposed security standards, namely, L0 and L1. Unfortunately, even today some devices are non-compliant with even the L0 security standard. About a year ago, a police complaint was filed regarding replay attacks by Axis Bank, eMudra and Suvidha Infoserve and show cause notices were served by UIDAI on the three agencies for violation of the Aadhaar Act[2], the L1 standard has still not even been published. Meetings between the government and mobile phone manufacturers to discuss the L1 standard has not resulted in any progress.

1.8. **Parallel Database and Black Market:** Since the value of compromised biometrics is permanent and will lead to a much bigger black market than that which exists for credit cards and debit cards because biometrics cannot be revoked. Yet, none of the parallel databases - State Resident Data Hubs, have been notified as Critical Information Infrastructure by the National Critical Information Infrastructure Protection Centre.

1.9. **Spatial privacy:** If face authorization is introduced as another level of security as is now being mooted, it will become possible to identify citizens in public places by installing high resolution cameras. Many persons except for those who have uploaded pictures onto social media can walk around public spaces without being easily identified. Many Indian citizens who serve in the intelligence agencies, military, law enforcement agencies do not upload their pictures into the public domain therefore it is not easily possible to identify them even if they are in public or semi-public spaces. If someone manages to compromise the CIDR – they will have this ability to identify persons of

[2]https://thewire.in/111869/indias-largest-biometric-database-turns-delhi-police-help/

interest to them in public places. Even otherwise, face recognition data once captured is open to misuse. There have been reports of the Chinese government using face recognition data to identify Uighur Muslims from its Xinjiang province and "fence them in" by a software that raises a red flag if profiled persons are seen more than 300 km outside their home locations.[3]

1.10. **Ownership**: The collection of biometric data blurs the line of ownership of data that forms an intrinsic part of the individual.For example, once a fingerprint or any other biometric information is provided to a requesting agency and is transmitted, then who owns the biometric data? Does the individual retain ownership over it or does the requesting agency have ownership over the data it has acquired. Aside from the question of ownership and legal rights, what is the degree of control the requesting agency retains over the biometric data it obtains for authentication

2. AADHAAR AND E-GOVERNANCE

From the perspective of reducing corruption and ensuring efficient and effective delivery of subsidies and services to eligible persons biometrics has several significant shortcomings.

2.1. **Exclusion during enrollment:** According to research that UIDAI responded to in the EPW – the margin of error increases with increase in size of the database and once the databases crosses one billion people (which it is claimed by UIDAI it already has) one out of every 146 people will be rejected during enrolment. These rejections according to UIDAI will be manually adjudicated by UIDAI staff without adhering to the principles of natural justice.

2.2. **Cost of creating Ghosts:** The UP ghost kit was sold at Rs. 5000/- and using this kit criminals were able to create multiple ghosts. Since there is no one outside the enrollment officer vouching for these ghosts there is no chain of trust and therefore nobody to hold accountable once a ghost has been discovered.

[3]https://www.bloomberg.com/news/articles/2018-01-17/china-said-to-test-facial-recognition-fence-in-muslim-heavy-area

2.3. **No recourse in terms of forgery:** The UIDAI claims that replay attacks will be dealt with just as the law deals with forged signatures. However, with the case of forged signature usually there is physical evidence that can be examined by experts appointed by the court but with replay attacks there is no evidence that can be accessed by the affected person during the process of seeking redress.

2.4. **Federal Governance:** The centralized use of biometrics militates against the constitutional principle of federal governance as it implicates the central government everytime the state government is trying to identify of authenticate a citizen. Decentralized identity management systems do not undermine the federal structure of Indian governance.

2.5. **Evidentiary value of biometrics in forensics:** When biometrics is used for inappropriate purposes like e-governance and when multiple actors have a copy of the biometrics [For ex. Gujarat State Resident Data Hub] it reduces the value of biometrics from a forensics perspective.

3. CENTRALIZED BIOMETRICS EVALUATED AGAINST PARTICULAR FUNDAMENTAL RIGHTS

3.1. **Centralized Biometrics and the Right to Privacy:** Biometrics impact bodily, spatial and informational privacy from the perspectives of the privacy principle of consent. By its very nature, biometric technology is consent neutral. Unlike a password which is private i.e. it is a secret locked away in the mind of the individual, biometric data, though personal, is out in the public. Biometric data can therefore be accessed and identification and authentication can be done - remotely, covertly and without the conscious cooperation of the human. For e.g. a) a person who is asleep b) a person who is unconscious and c) and person who is dead.

3.2. **Biometrics and the Right to Dignity [as part of the right to life]:**, The staff of the enrolment agencies and also staff of the KUAs and AUAs who are usually men and not government officials are touching the bodies of persons - of women, elderly persons, children, sexual minorities and other vulnerable persons, e.g. holding their hands to press down and obtain fingerprints. Evidence: photographs on the UIDAI Twitter Feed. Other identification technologies like smart cards do not subject persons to such indignities.

3.3. **Biometrics and the Right to Equal Treatment under Law:** The reports of exclusion that have emerged from different sources such as the "State of Aadhaar Report" [produced purely using government data] demonstrate that biometrics discriminate in at least three significant ways. Even though the Aadhaar Act has exceptions for these vulnerable populations it would be better to opt for a technology that did not discriminate against the weak, such as smart card technology.

1. **Age:** The biometrics of aged persons and children change with time and therefore are less reliable than those of persons in their youth and middle-age.
2. **Class:** The biometrics of persons engaged in manual labour is not as reliable as those who are not engaged in manual labour.
3. **Ability:** The biometrics of persons who are disabled are not as reliable as those who are able.
4. **Illness:** There are many diseases of the hands and the eyes that affect the reliability of biometric technology such as leprosy, cataract etc.

It is submitted that given the degree to which biometric technology impacts fundamental rights, it is best reserved for fighting terror and crime and is inappropriate for everyday interactions between the state and law-abiding citizens.