The Government of India Hired Foreign Corporations to Act as 'Biometric Service Providers": Role of CIA in the Aadhaar Database Exposed in Supreme Court

By Shelley Kasli
Asia-Pacific Research, March 17, 2018

Region: South Asia
Theme: Justice, Politics

Last year we at GreatGameIndia had exposed how spies of Central Intelligence Agency (CIA) of the United States of America had access to the Aadhaar database through a CIA front company Crossmatch contracted by Unique Identification Authority of India (UIDAI) for enrollment and capturing of biometrics of Indian citizens. The issue was raised in the Rajya Sabha by ***Sukhendu Sekhar Roy****.*

.

.

> Has the CIA already stolen India's #Aadhaar database? https://t.co/hFcALy2Lki #modi
>
> — WikiLeaks (@wikileaks) August 25, 2017

Today, this critical issue of threat to our National Security posed by the Aadhaar project was raised in the Supreme Court by senior counsel ***Anand Grover*** *on behalf of the petitioner* ***Colonel (retd.) Mathew Thomas****. Below are the relevant excerpts from writ petition in possession of GreatGameIndia that exposes the role of foreign intelligence agencies in Aadhaar project.*

Contracts with Foreign Agencies render the Aadhaar 'insecure ab initio'

It is submitted that of the identity information collected under the Aadhaar Project was compromised at the inception. In that sense, the Aadhaar system is a prime example of a technological system being **"Insecure Ab Initio"**. It is submitted that Aadhaar system is *insecure ab initio* for the following reasons:

- That foreign corporations were engaged to build the Aadhaar system, giving them complete access to all Aadhaar-information and continuing control over the Aadhaar technology; and
- That the Aadhaar-data was diverted into non-secure destinations before even it entered the CIDR.

The Government of India engaged foreign corporations to act as 'Biometric Service Providers' (hereinafter "BSPs"), who built the underlying technology on which the Aadhaar system now runs. In 2010, at the inception of the Aadhaar project, contracts were awarded to different foreign based BSPs for the 'design, supply and implementation of the biometric solutions to be used by the UIDAI to set up the Aadhaar infrastructure', which included L-1 Identity Solutions Operating Company Private Limited (hereinafter "L-1 India").

L-1 is the Indian subsidiary of L-1 Identity Solutions Operating Company (hereinafter **"L-1, US"**), a company incorporated in Delaware, USA. A copy of the contract between L-1 India and the President of India acting through the UIDAI, dated August 24, 2010, sets out the commercial and technical understanding between the UIDAI and L-1 for the development of the Aadhaar system.

As per the Contract, L-1 Company was to operate in its capacity of a "Biometric Solution Provider", i.e. it would provide for design, supply and implementation of biometric matching services. Particularly the scope of work under the contract included providing design, supply, install, configure, commission, maintain and support multi-modal Automatic Biometric Identification Subsystem (ABIS), multi-modal software development kit for client enrolment station, verification server, manual adjudication and monitoring function of the UID application. The Contract was initially valid for a period of two years or till the completion of 20 crore enrollments, whichever was earlier.

Hence, L-1 Company was licensed to provide technological solutions not just at the stage of enrolment, i.e. collection of core biometrics information (fingerprint and Iris scan), along with demographic details, but also in the process of de-duplication and also 1:1 authentication.

- **L-1 Company had access to sensitive personal information of Indian residents**

The said contract further discloses that L-1 had access to identity information and related information, of Aadhaar enrollees, and had continuing control over the Aadhaar technology. Further, at the time of signing the contract and during the term of subsistence of the contract there was no applicable law governing the Aadhaar project or data protection. In this context, reference to relevant portions of the contract are made below.

Clause 15.1 of Annexure A of the Agreement between the UIDAI and L-1 India (hereinafter "BSP Agreement") states: *"By virtue of this Contract, M/s L-1 Identity Solutions Operating Company may have* ***access to personal information of the Purchaser and/or a third party or any resident of India****, any other person covered within the ambit of any legislation as may be applicable. The Purchaser shall have sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the residents of India that may be in the possession of M/s L-1 Identity Solutions Operating Company or the Team of M/s L-1 Identity Solutions Operating Company in the course of performing the Services under this Contract."*

From the abovementioned Clause 15.1, it is evident that the L-1 (the US parent company) had access to the personal information of UIDAI, including the Aadhaar data submitted by Indian residents wishing to enroll for Aadhaar. The personal information as mentioned above would include the fingerprint, iris, face photograph and demographic information, or any data such as verifying documents of the nature of passport copy, PAN card copy etc. This

represents an unacceptable breach of confidentiality and privacy with regard to the intimate data of Indian residents, including biometric data.

Further Clause 4.1.1 (1) of Annexure E of the BSP Agreement confirms that L-1 had access to the biometric and demographic data of Aadhaar enrollees. The said provision reads as follows:

"4.1.1 Multi-modal Biometric de-duplication in the Enrolment Server

Considering the expected size of the de-duplication task, the UID enrolment server will utilize:

- *Multi-modal de-duplication. Multiple modalities – fingerprint and iris will be used for de-duplication. Face photograph is provided if the vendor desires to use it for deduplication. While certain demographical information is also provided, UIDAI provides no assurance of its accuracy. Demographic information shall not be used for filtering during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UID program. Each multi-model de-duplication request will contain an indexing number (Reference ID) in addition to the multi-modal biometric and demographic data. In the event one or more duplicate enrolments is found, the ABIS will pass back the Reference ID of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100] with 0 indicating the least level of similarity and 100 as the highest level of similarity."*

Clause 4.1.1 of Annexure E of the BSP Agreement indicates that each de-duplication request contains all of the relevant Aadhaar data, including demographics and biometrics, and therefore the BSP has access to this data to complete the de-duplication task. Such data is not encrypted, but provided in raw form, as the de-duplication process requires unencrypted data in order to facilitate the comparative check as encrypted data cannot be used for de-duplication.

This is reinforced by **Clause 9.8.2** of Annexure E of the BSP Agreement, which deals with the 'Data Quality Monitoring and Reporting' obligations of the BSPs. Per this provision, the BSP is required to continuously monitor the quality of the data, which entails directly analyzing the Aadhaar data in raw form. Reference is made to the second paragraph of the aforementioned clause on page 53 of Annexure E, which states that: "*Data quality of capture would be received with the image. Image would be received in raw form.*" Here, the term image refers to the scanned captured of the biometrics of Aadhaar holders, i.e. fingerprint, iris and facial photograph.

This proves beyond doubt that the BSPs had access to the biometric data of the Aadhaar holders in raw form, and the demographic information of all Aadhaar holders.

The provision of access to Aadhaar data, to BSPs is further confirmed in *Clause 3 of Annexure B of the BSP Agreement*, which states that: *"In the course of the Agreement, the Biometric Solution Provider may collect, use, transfer, store or otherwise process (collectively, "process") information that pertains to specific individuals and can be linked to them ("personal data"). Biometric Solution Provider warrants that it shall process all personal data in accordance with applicable law and regulation."*

This clause confirms that the foreign BSPs had access to personal information gathered from Indian residents under the Aadhaar project. Pertinently, at the time of execution of the BSP Agreement, there was no Aadhaar legislation or data protection legislation in India.

(ii) That the BSP Agreement allowed the BSPs to retain data for unreasonably long period of time

Clause 15.3 of Annexure A of the BSP Agreement states that:

"The Data shall be retained by M/s L-1 Identity Solutions Operating Company for not more than a period of 7 years, as per the Retention Policy of the Government of India or any other policy that the UIDAI may adopt in the future."

Similarly, Clause 14.2 of Annexure A of the BSP Agreement allows retention of any documents arising out of the agreement for a long period of time. The Clause states that:

"The Documents shall be retained by L-1 Identity Solutions Operating Company not more than a period of 7 years as per Retention Policy of Government of India or any other policy that UIDAI may adopt in future"

Clearly, the BSP Agreement allowed the foreign BSP to retain identification information and documents collected during the process of enrolment for 7 long years. This is an unreasonable time period for the retention of such data, given that the BSP Agreement was valid initially only for a period of 2 years or completion of 20 crore enrollment transactions, whichever would have been earlier.

(iii) The BSP Agreement facilitated access to personal information by allowing local storage of data

It is submitted that the Contract provided for localized storing of the information collected from residents coming for enrolment. That is, the information collected by L-1 Company in its capacity as the Biometric Service provider was not shared with the Central Information Data Repository in real-time. Instead, the enrolling software was to enroll the *"residents in the field and upload the data onto the server in batch mode"*. This implies that the enrolling agencies had to store the biometric and demographic data locally before it was uploaded on the server.

Such storage of biometric information of enrollees was facilitated by a reference database. The BSP Agreement provided that each enrolling system- Automated Biometric Authentication System (ABIS), *"shall maintain its own database of indexed biometric references (called reference database) as well as synchronized disaster recovery database at a separate physical location. This reference database is separate from UID database that is outside of ABIS and not accessible to ABIS. All information necessary for ABIS to perform its functions is maintained by ABIS in the reference database"*.

It is further submitted that the Contract required L-1 Company to maintain a copy of the reference database at a separate location. This clearly indicates that multiple copies of the sensitive private information of Indian residents were available at separate locations. Hence, even if it is argued that the enrolling agencies/systems did not have direct access to the data stored in the central UID database, now known as the CIDR, the BSP Agreement enabled third parties to have access to personal data of enrollees by very provision for a localized reference database.

Further, there is nothing in the contract relating to the destruction of the data retained in this manner, and certification of such deletion. It is submitted that even the present Aadhaar Act contains no provision that relates to the data in these databases.

(iv) Members of the Board of Directors of the BSP were related to Foreign Intelligence Services

It is submitted that some former members of the Board of Directors were a part of the US intelligence agency. For instance, Louis J. Freeh served as a Director of L-1 Identity Solutions Inc. from July 24, 2006 to August 30, 2007. He had previously served as the Director of the Federal Bureau of Investigation from 1993 to 2001. Further, from July 10, 2006 to 2011, Mr. James M. Loy served as a Director of MorphoTrust USA, Inc. He was also served as Deputy Secretary of U.S. Department of Homeland Security from December 4, 2003 to March 2005. Another former director of L-1 Company, George Tenet (who served at L-1 Company from December 2005 to June 29, 2008) was also a former Chief of the **Central Intelligence Agency**.

It is clear that the BSP Agreement indicates that L-1 had access to confidential Aadhaar data. Under the provisions of the USA Patriot Act, 2001 and the Foreign Intelligence Surveillance Act, 1978, the US Government and Intelligence Agencies can legally require a US based corporation to handover information that it either owns or has access to, and this would extend to the Aadhaar data covered in the scope of the BSP Agreement.

Further, in 2009, **Safran, a French defence conglomerate in which the French Government had a stake, acquired Morpho, a US company that provided biometric service solutions. The UIDAI signed contracts with both L-1 and Morpho in 2010.** A few weeks after the execution of the BSP Agreement, L-1 was acquired by Safran and merged with its subsidiary Morpho. Currently, L-1 is owned by an assortment of private equity investors, and operates under the name IDEMIA Identity and Security.

Moreover, personnel of the foreign BSPs continue to be employed by the UIDAI as of January 2018, as indicated by the data that is available on the 'attendance.gov.in' portal – which discloses this.

The Aadhaar technology, and particularly the algorithms used in ABIS and the Aadhaar de-duplication continue to remain an absolute black-box in that neither the UIDAI nor the Government has control over the technology or understands exactly how it works; this is proprietary technology that is merely under a perpetual license to the UIDAI.

Hence, given that any data collected during the process of enrolment and/or use of

Aadhaar number was:

1. Accessible to foreign BSPs through the whole Aadhaar pipeline;
2. Diverted to various State Resident Data Hubs, and Registrar Local Databases, and Enrolling Agency local devices;

the identity information and related data of Aadhaar enrolled Indian residents is ***"insecure ab initio"***.

*

This article was originally published on GGI News.

***Shelley Kasli** is the Co-founder and Editor at GreatGameIndia, a quarterly journal on geopolitics and international affairs. He can be reached at shelley.kasli@greatgameindia.com.*

Featured image is from the author.
