AFFIDAVIT

I, Samir Kelekar s/o Gurunath Kelekar, aged about 53 years and resident of xxxxxx hereby solemnly affirm and declare that :-

1. That I have working experience of more than thirty (30) years in the field of IT and about 15 years of experience in the field of cyber security and that currently I am heading a company which I founded for the purpose of providing security solutions to organisations which need to protect themselves against Internet / Cyber / digital frauds.

2. That my firm's name is M/s. Teknotrends Software Pvt. Ltd.

3. That I graduated in electrical engineering from the Indian Institute, Mumbai (IIT, Mumbai) in 1983. Thereafter I obtained a post-graduate degree in Computer Engineering from Clemson University, South Carolina, USA.

4. That I hold a doctorate degree (PhD) in electrical engineering from Columbia University, New York, USA.

5. That I have done work for clients, including, Canara Bank, G E Health and MTN, a multi-national South African mobile phone company.

6. That I am aware that the Government of India is implementing "UID / Aadhaar" based authentication for various government services and that private entities may also use the UID / "Aadhaar" database for identifying individuals.

7. That I am aware that there are petitions before the Hon'ble Supreme Court of India challenging the said UID/ Aadhaar project on various ground, inter alia, that the said project poses a constitutionally impermissible danger to citizens' basic civil liberties including their privacy and I hereby allow this affidavit to be placed by one or more of the petitioners in support of their challenge on the said grounds to the said project.

8. That as someone with fairly extensive experience of cyber security, I can categorically state that this project is highly imprudent, as it throws open the clear possibility of compromising basic privacy by facilitating real-time and non-real-time surveillance of UID holders by the UID authority and other actors that may gain access to the authentication records held with the said authority or authentication data traffic as the case may be.

9. That I state that I have perused the documents that UIDAI have put out in relation to the design of the Aadhaar authentication system, and I can categorically state that it is quite easy to know the location and type of transaction every time such authentication takes place using a scanner for fingerprints or iris and the records of these in the UID / "Aadhaar" database.

10. I state that it is not dissimilar to knowing the place from where a person made a call using his / her mobile phone. Just as the mobile phone connects to a tower from where the phone signals are sent to other towers and the servers of the

mobile phone companies, biometric scanners also have SIMs and IP Addresses to locate the place from the transaction took place and its nature. Any administrator of the UIDAI server or any employee or other person with access to transaction data, with a little help from the servers (Authentication User Agents and Authentication Server Agents, as they are called in UIDAI literature), through which authentication request is sent to the UIDAI, will be able to track the transaction and the person carrying out the same. Further, I also point out that UIDAI recommends that each point of service device i.e. the device from which an authentication request emanates, register itself with the UIDAI and acquire for itself a unique device id, which shall then be passed to the UIDAI along with the request for every authentication transaction. I state herein that the said method of uniquely identifying every device and being able to map every authentication transaction to be emanating from a unique registered device, further makes the task of tracking down the exact location and place from which an authentication request emanates easier.

11. I further state that there are technical tools that are available that make it easy and possible to track the electronic path that authentication requests from any given authentication device to the Central Identification Data Repository take as part of their authentication transaction.

12. I further wish to point out that today, it is well known that no security is perfect. The idea is to design a system where in in case of a breach, the damage is minimal and backups are available. Hence, passwords should be changeable. Biometrics as a password is problematic in that it cannot be changed if stolen / lost / hacked.

13. That secondly, a centralized database has the problem that once hacked all data can be lost. Specifically, consider if the Army personnel use this as an

authentication mechanism before getting their salaries. The location from which they authenticate can be found as it will be done via a scanner which has an IP address / is on a mobile internet. From the tower to which the scanner connects via its SIM card, its location can be found. This data will be available in the logs of the Aadhaar system. Any compromise of the Aadhaar system means that the hackers can know the exact location of each army personnel of the country at the time when they take their salary. This can be a big risk to national security, and this is just one example as to why it is, in my opinion, imprudent to use such a system.

DEPONENT

VERIFICATION

I, the deponent above-named, hereby solemnly declare and affirm that the contents of this affidavit in paragraphs 1 through 13 are all true and correct to the best of my knowledge and nothing material is concealed therefrom.

Verified on ________________ day of April 2016.

DEPONENT