PRESS INFORMATION BUREAU
पत्र सूचना कार्यालय
GOVERNMENT OF INDIA
भारत सरकार

**Economic Times , Delhi**
**Sunday, 14th January 2018; Page: 7**
**Width: 65.46 cms; Height: 76.72 cms; a3; ID: 21.2018-01-14.16**

R Sriram

# The Silly Scare Tactic

## The chant that Aadhaar will enable state surveillance is malicious propaganda

Hollywood may be worried over sexual harassment scandals these days but seven years ago, it was caught bang in the middle of a hacking scandal. Few may remember now, but a hacker spent many months taking down and controlling email accounts of celebrities like actor Scarlett Johansson and singer Christina Aguilera. He ferreted out private photographs, copied them to a folder on his computer and released them widely online, causing acute embarrassment, outrage and pain to the victims. It was caused by a simple hack because the victims had been foolish enough to leave enough personal information on social media websites which the hacker used to generate passwords and enter their accounts.

**Aadhaar has got nothing to do with surveillance or snooping.** It is not a spy software or system that reads your emails, conversations or extracts your financial data from banks

This was in 2011. It is 2018 now and two things have happened simultaneously as far as online privacy debate is concerned. One, hacking has become increasingly sophisticated and effective. Two, the amount of personal, individual information available publicly has risen manifold. Not only are personal details widely available on social media networks, basic information about an individual can be accessed easily. Scour the internet for voters' list and you will come up with all the information you want: name, address etc.

### No Access

It is important to keep all this in mind amidst the raging debate over Aadhaar, which has been dubbed a fascist tool, a surveillance mechanism to enslave Indians and a project that leaks like a sieve and cannot be trusted. The fact that the Supreme Court will begin final hearings on January 17 on the validity of Aadhaar may just be a coincidence as to why we are having this debate now. Or, it may not be. Needless to say, there is a lot at stake.

The key issue about Aadhaar has always been the safety and security of its biometric data. Remember, the debate is not about public data like name, date of birth, address etc. It is the biometric fingerprint scan and iris scan that is the focus of everybody's attention. This is the personal data, which if hacked or violated, would be a very serious issue. Anti-Aadhaar activists say this is a surveillance state mechanism and should not be trusted. They allege that it is a tool to keep track of your financial dealings and movements. Having spent some time in understanding how Aadhaar architecture and security works with experts, I can categorically say that this is bunkum! Aadhaar has got nothing to do with surveillance or snooping. It is not a spy software or system that reads your emails, conversations or extracts your financial data from banks. It is not designed to track an individual's movements or personal or financial transactions. Calling it a surveillance state is a deliberate scare tactic, a mischievous and malicious propaganda, one that Dr Joseph Goebbels would have been very proud of! Aadhaar also does not store any financial or personal information. It is not designed that way at all. The linking of my bank account to Aadhaar does not in any way give UIDAI or its officials access to my financial records. They don't know what I do in my bank account, what products I buy or what services I use.

The second aspect of Aadhaar, not widely discussed or widely known, is that the biometric data is not accessible through the internet. It can only be physically accessed and even then it is difficult to link the biometrics with a particular individual. The UIDAI system has compartmentalised data storage which would make it very difficult for a hacker or a raider to accurately identify individuals with just one set of information. For instance, in order to link the biometrics with an Aadhaar number, you not only need to have the Aadhaar number, but also the reference/registration number given at the time of enrollment. The job of the hacker, needless to say, becomes very difficult.

### UIDAI Vaults

The physical-only access to biometric database is buttressed by the limited communication between the identification interface and the service provider. A bank, which sends request for identification to UIDAI database, gets only a yes or no answer. There is no transfer of images or data back to the service provider. Nor can the service provider get full access to the image stored deep in the UIDAI vaults. Only a sample of the image is used for identification purposes while the full image is stored in a place without internet access.

**The biometric data is not accessible through the internet.** It can only be physically accessed and even then it is difficult to link the biometrics with a particular individual

No system is free from glitches or troubles. A big negative side effect of Aadhaar has been the tragic tales of denial of service in hospitals or of food grains to the needy. Governments and local bodies across the country must work together to ensure that such tragedies are not repeated. There surely must be a method to ensure that identities other than Aadhaar are used in emergency cases and that service is provided to the needy.

Goebbels said that if you tell a lie big enough and keep repeating it people will eventually come to believe it. The anti-Aadhaar crowd with its alarmist propaganda of state surveillance seems to have taken the Nazi leader's advice to heart. Time to call their bluff. ■