

20.02.2018



10 Myths on Aadhaar Debunked

AJIT SINGH

Aadhaar is gradually becoming an [essential document](#) for the proof of identity and the proof of address. Owing to its importance, a number of myths are being circulated against the usage of Aadhaar. Today, we are going to uncover the truth behind some of the myths spread about the safety and security of Aadhaar:

1. Aadhaar data is used for surveillance purpose by the government.

According to the Section 32(3) of the Aadhaar Act, 2016, UIDAI is prohibited from collecting, maintaining or controlling any information related to the Aadhaar holder apart from your biometric (photograph, fingerprints and iris scan) and demographic details (name, DoB, gender and address). UIDAI is not authorised to store any other details at all. Once you [link Aadhaar with PAN](#), it becomes important to link it with all other bank accounts, mobile numbers and other such instruments for verification purpose and UIDAI is not authorised to store data associated with these schemes and instruments.

2. Account details are shared by banks to UIDAI

Rumours have been spread regarding the sharing of bank account details such as bank statements, money in the account, transaction details, etc. by banks to UIDAI. **UIDAI is not authorised** to request for such information from banks and banks are not liable to provide any of these details to UIDAI. When carrying out verification of your bank account, banks only share the Aadhaar number, biometric provided by the account holder and name to UIDAI.

Your bank account details are not sent to UIDAI whatsoever. In case the information provided by the bank matches with the data provided to UIDAI by the Aadhaar card holder during enrolment, UIDAI replies with “Yes” affirming that the data provided by the individual is correct. However, in some cases, your basic KYC details such as name, DoB, photograph, etc. are sent to the service provider.

3. Bank accounts can be hacked if a person knows the Aadhaar number

Your bank account has to be linked with Aadhaar to prove the authenticity of the bank account. Even if one knows your Aadhaar number that is linked with your bank account, he will not be able to access your account details. If one wants to check the bank account linked with Aadhaar, he has to enter the OTP sent to the mobile number registered with UIDAI. Hacking bank accounts through UIDAI is next to impossible as no bank details are stored with the organisation.

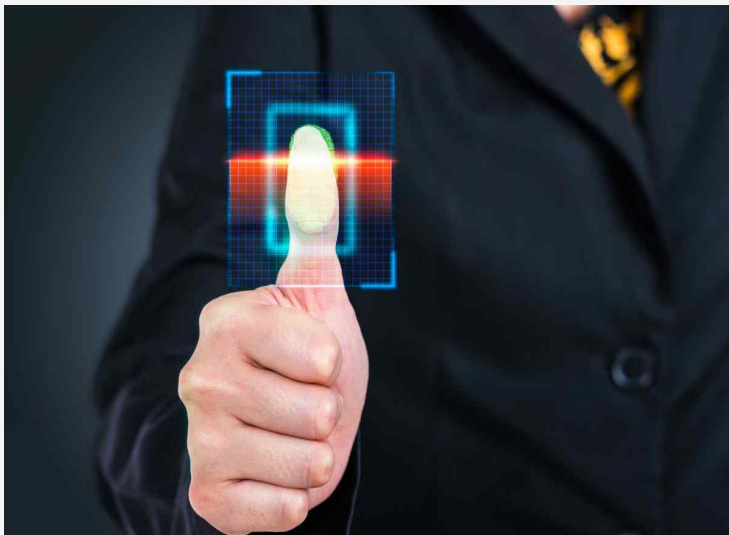
4. The government is suspecting all by asking to link bank accounts with Aadhaar

The government is laying out robust and authentic methods to curb the menace of black money and corruption. Linking of bank accounts with Aadhaar is one such step in the direction to cleanse the Indian economy. A number of bank accounts have been opened under fake identity and are being used to fund anti-social elements, hawala transactions, operational malpractices, etc. Bank accounts not linked with Aadhaar will be deactivated post the deadline and the money accumulated in those accounts would be seized after some time. Genuine bank accounts will keep on functioning as usual without any intrusion by the government. There are no plans to snoop on

bank accounts of people by making it mandatory to link bank accounts with Aadhaar.

5. It will be easier for the government to intrude the privacy after mobile verification

A number of cases had come to the forefront where terrorists and anti-social elements used SIM cards issued on fake identity to carry out misadventures in India. Owing to it, the government made [linking of mobile numbers with Aadhaar](#) mandatory through biometric re-verification. Neither UIDAI nor Telecom Service Providers (TSPs) can breach their area of authorised access and store or request data. Thus, no privacy of the individual will be compromised with in any case. In case any such activity is brought into notice, stringent action would be taken by the government after proper investigation.



No TSP has the authority under its domain to store biometrics and other data of the subscriber taken for mobile re-verification using Aadhaar.(Photo: iStock)

6. Mobile companies store biometrics and other data to use it for other purposes

No TSP has the authority under its domain to store biometrics and other data of the subscriber taken for mobile re-verification using Aadhaar. All data collected has to be directly transferred to UIDAI for verification. In case any TSP stores any of the data, it will be severely penalised. The government continuously monitors the re-verification process to prevent potential violators from carrying out such malicious activities.

7. Aadhaar linking is mandatory for NRIs as well

Aadhaar linking with various documents is mandatory for all residents of India, be it Indian citizens or foreigners. However, people such as NRIs, OCIs or PIOs, who do not reside in India, are not eligible for an Aadhaar. Thus, such people do not have to link different instruments with Aadhaar.

8. Poor and downtrodden are denied services due to lack of Aadhaar

According to the Section 7 of the Aadhaar Act, 2016, no individual can be denied any benefits provided by the government if he has not been assigned an Aadhaar. In case any government body denies providing benefits to the beneficiary on the pretext of not having Aadhaar or any technical error, a complaint would be lodged against higher authorities of the department.

9. e-Aadhaar is nowhere accepted by agencies

e-Aadhaar is a valid proof of identity or residence and is accepted by all government bodies. In case a person has to submit Aadhaar, he can print the e-Aadhaar and submit a copy to the authorities. People can update Aadhaar data and download the e-Aadhaar after [checking the Aadhaar status online](#). The e-Aadhaar copy has the updated address and other details of the individual, thus it should be preferred by all instead of the old Aadhaar card.

10. Aadhaar data of millions is easily available online.

A lot of mis-reporting is being carried out regarding Aadhaar. Recently, a fake news was circulated stating that Aadhaar data of millions was available online for just 500/-. Appropriate action was taken against those involved in the issue. In a history of more than 7 years, no such authentic instance of Aadhaar data breach has come into the picture. UIDAI has employed state of the art technology and is continuously upgrading its systems to keep the data safe and mitigate any such threats of data thefts.