Aarogya Setu App and Privacy Concerns

June 23, 2020

The Ministry of Home Affairs' (MHA) directive to make the Aarogya Setu app mandatory for individuals in all workplaces has raised suspicion with privacy advocates who feel the app has several security-related blackholes and can eventually become surveillance tools for the government.

Aarogya Setu App

To combat the coronavirus pandemic, the government of India has launched a new app. Called Aarogya Setu, the new **coronavirus tracking app** warns users if they have crossed paths with any infected people recently. The app has been developed by the central government and **NIC eGov mobile apps**. As the app is based on location and users' data, to make it work properly, the app requires **more data from different locations.**

The privacy policy of the app is **completely silent on what security practices** are being followed. Also, there is a huge gap in privacy policy, as it does not tell what is being done with the data that is being collected every 15 minutes.

Concerns Regarding the App

- India is currently the only democratic nation in the world that has made its coronavirus tracking app mandatory for people.
- It collects **multiple data points for personal and sensitive information** which increases privacy risks.
- It's **code is not open source** and thus the code and methods can't easily be reviewed by third parties.
- Researchers and individual users cannot actually check if the government has deleted people's personal

information and there is **no means of transparently auditing** what the app is doing in the backend.

- The **liability clause** in the app’s Terms of Service **exempts the Government** from liability in the event of any unauthorised access to the (user’s) information or modification thereof, meaning there is no liability for the Government even if personal information of users is leaked.