Concerns with Aarogya Setu App

What is the issue?

- The Centre recently made the Aarogya Setu app mandatory for both public and private sector employees and for travellers on public transport systems.
- Though it is made in light of the COVID-19 pandemic, serious data security and privacy concerns are attached to the system.

How does the Aarogya Setu app work?

- The App continuously collects data on the location of the user and cross-references it with the Central government database.
- The application asks for the name, phone number, profession, gender, age and a list of countries visited in the past 30 days.
- It asks whether the user wants to be informed if they have crossed paths with someone who has tested COVID-19 positive.
- The application allows the users to self-assess their symptoms.
- It then compartmentalises them into different groups based on their COVID-19 risk.
- By switching on GPS location and Bluetooth, it monitors the location of the user, and the proximity to other Bluetooth-on devices.
- [The app requires the Bluetooth and GPS Location sharing turned on at all times.]
- By using big data, the app will supposedly be able to check for contact tracing if a given handset has been in a “red zone”, or near the handset of a user marked infected.
- It uses colour coding to mark the user as healthy, infected, or recovered.

What are the concerns?

- **Exclusion** - New smartphones will come with the app pre-installed.
- The app can be used only on a smartphone.
- Roughly, half of India’s one billion mobile subscribers do not use smartphones or data connections.
- This segment is largely the lower-income group.
- These subscribers would not be able to download the app and would, therefore, be excluded from availing of public transport, or working.
- **Security** - The security concerns arise from the fact that the app was put

together in haste and the code is not open-source.

- [This is unlike similar contact-tracing apps released in Singapore and South Korea.]
- This means that its security, or problems in programming, cannot be independently verified.
- Being a surveillance app, it could gather vast amounts of data far beyond what is required for the stated narrow purpose of contact tracing.
- It gathers huge amounts of critical private data.
- But the lack of open-source programming makes it difficult to judge what data it may be collecting.
- In addition to location, it may, for instance, be monitoring phone calls, or SMS details.
- It may be reading social message posts and WhatsApp messages.
- The data is transferred to servers, which may or may not be secure.
- Technical details about anonymisation are unknown.
- There is also lack of clarity about which agency would be responsible in the case of data theft.
- **Privacy** - The breach of privacy involved in forcing such an intrusive app upon every smartphone is thus a prime concern.
- One of the guiding principles in collecting private data is to gather the minimum required for a specific purpose.
- It should ask granular permission for every separate data gathering.
- Another important principle is giving citizens the "right to forget".
- Unfortunately, India still does not have a personal data protection law incorporating such provisions.
- This is despite privacy being acknowledged as a fundamental right since 2017.
- In all, in the absence of specific legislation, the app may be misused and citizens should not be forced to download it.

Source: Business Standard, The Week