Aarogya Setu App and security issues

Part of: GS Prelims and GS-III-Internal security

- Aarogya Setu app has been launched by the Ministry of Electronics and Information Technology.
- It will help people in identifying the risk of getting affected by the CoronaVirus.
- It will calculate risk based on the user’s interaction with others, using cutting edge Bluetooth technology, algorithms and artificial intelligence.
- Once installed in a smartphone, the app detects other nearby devices with Aarogya Setu installed.
- The App will help the Government take necessary timely steps for assessing risk of spread of COVID-19 infection, and ensuring isolation where required.

Key Issues

- The key issue is there is not enough information available on what data will be collected, how long it will be stored and what uses it will be put to.
- No specification on the issue of how the government will use data if the data gets shared with the government of India.
- On the data retention part, the app’s privacy policy specifies only the data available on the app and does not specify for how long the Government of India will retain server side data.
- Additionally, there was also a question of proportionality with the app and whether it will be as effective as envisaged in containing the Covid-19 outbreak.
  - India’s situation is different from countries like Singapore, where a good number of people have smartphones.
  - In India compared to its population, smartphone users are very less which means very few people will be able to download the app.

Way Forward

- The app privacy policy needs detailed clarification on data collection, its storage and uses.
- The Government of India must specify how it will deal with the app’s data and how long it will retain the server side data.
- According to the Supreme Court in the Puttaswamy judgement (2017), the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy.

Privacy Judgement

Context

- Two years ago, in August 2017, a nine-judge bench of the Supreme Court in Justice K. S. Puttaswamy (Retd) Vs Union of India unanimously held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21.
- It held that privacy is a natural right that inheres in all natural persons, and that the right may be restricted only by state action that passes each of the three tests:
First, such state action must have a legislative mandate; 
Second, it must be pursuing a legitimate state purpose; and 
Third, it must be proportionate i.e., such state action — both in its nature and extent, must be necessary in a democratic society and the action ought to be the least intrusive of the available alternatives to accomplish the ends.

Privacy Judgement as a guiding tool

- This landmark judgement fundamentally changed the way in which the government viewed its citizens’ privacy, both in practice and prescription.
- It requires governments to undertake structural reforms and bring transparency and openness in the process of commissioning and executing its surveillance projects, and build a mechanism of judicial oversight over surveillance requests.
- It demands from the authorities to demonstrate great care and sensitivity in dealing with personal information of its citizens.
- It requires to legislate a transformative, rights-oriented data protection law that holds all powerful entities that deal with citizens’ personal data (data controllers), including the state, accountable.

Steps taken by Government to strengthen Privacy Regime

- Government appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna that submitted its report in July 2018 along with a draft Data Protection Bill
  - The Report has a wide range of recommendations to strengthen privacy law in India. Its proposals included restrictions on processing and collection of data, Data Protection Authority, right to be forgotten, data localisation, explicit consent requirements for sensitive personal data, etc.
- Information Technology Act, 2000: The IT Act provides for safeguard against certain breaches in relation to data from computer systems. It contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein.

Two Years of Privacy Judgement

The judgment in K.S. Puttaswamy effected little change in the government’s thinking or practice as it related to privacy and the personal data of its citizens.

- National Security Vs Privacy: Government continued to commission and execute mass surveillance programmes with little regard for necessity or proportionality, with justifications always voiced in terms of broad national security talking points.
  - The Ministry of Home Affairs, in December 2018, authorised 10 Central agencies to “intercept, monitor and decrypt any information generated, transmitted, received or stored in any computer in the country”. This notification is presently under challenge before the Supreme Court.
  - In July 2018, it became known that the Ministry of Information Broadcasting had floated a tender for ‘Social Media Monitoring Hub’, a technical solution to snoop on all social media communications, including email. The government had to withdraw the project following the top court’s stinging rebuke.
  - A request for proposal for a similar social media surveillance programme was floated in August 2018 by the Unique Identification Authority of India (UIDAI), which is
presently under challenge before the Supreme Court.

- The Income-Tax department has its ‘Project Insight’ which also has similar mass surveillance ends.

- **Data use Vs Privacy:**
  - The government has shunned a rights-oriented approach in the collection, storage and processing of personal data and has stuck to its ‘public good’ and ‘data is the new oil’ discourse.
  - This is evident from this year’s Economic Survey as it commends the government for having been able to sell and monetise the vehicle owners’ data in the Vahan database and exhorts it to replicate the success with other databases.
  - The Draft Personal Data Protection Bill that urged for a ‘free and fair digital economy’, has the digital economy as the end and the notion of privacy merely being a shaper of the means.

👍 Jai Hind Jai Bharat