The Problem with Private Play in Facial Recognition Technology (FRT)

What is the issue?

Clearview AI, an American facial recognition company has scraped images from across the Internet to design a powerful facial recognition tool, rekindling the debates on the private play in FRT.

What is FRT and how does it work?

- FRT is a system for automated matching or identification of faces usually using a database representing facial characteristics.
- Technologies vary, but the basic steps in working of a FRT are as follows.
- **Step 1- Capture**- A picture of a face is captured from a photo or video.
- **Step 2**- **Extraction**- Facial recognition software reads the geometry of the face.
- Key factors include the distance between the eyes and the distance from forehead to chin. The software identifies facial landmarks producing in facial signature.
- **Step 3**- **Comparison**- The facial signature which is a mathematical formula is compared to a database of known faces.
- **Step 4- Matching-** A determination is made depending upon the matching of the faceprint with an image in a facial recognition system database.

What is the significance of FRT?

- To identify criminals, missing people, and unidentified dead bodies as used in CCTNS
- To prevent the use of fake citizen IDs by fraudsters, infiltration of terrorists, illegal immigrants,etc.
- For easier and automatic identification and doesn't need huge manpower
- Use of NAFRS eases the checking procedural delays in airports

Has it been deployed previously in India?

- In August 2018, Telangana police launched their own facial recognition facility.
- Ministry of Civil Aviation's **"DigiYatra**" has used the facial recognition system, on a trial basis in Hyderabad airport.
- NCRB's Crime and Criminal Tracking Network & Systems **(CCTNS**) uses automated facial recognition to identify suspects of a crime, monitor crowded areas during festival times for habitual offenders, and find missing children.
- In more extreme cases, like the reported use by the Lucknow police, FRT is even being deployed to identify women in distress through their facial expressions and, apparently to keep them safe.
- To empower the Indian police with information technology, India has approved the implementation of National Automated Facial Recognition System (NAFRS).

What are the risks associated with the use of FRT by private players?

- **Privacy risks-** Since FRT relies on vast amounts of datasets, it is unclear how these are being made available to private players.
- The public does not know if the government has entered into data sharing agreements for this purpose.
- It might compromise the informational autonomy that the Supreme Court read in the fundamental right to privacy in the Puttaswamy judgment.
- There is an absence of any information on what personal (including biometric) information is being shared and to what end under FRT procurement.
- **Role of private enterprises**-It is unclear as to whether the role of private enterprises is merely to develop FRT, or to even help in deployment and upkeep.
- It raises doubt on whether the surveillance functions of the state might get transferred to a private citizen or entity.
- **Legal liability**- The potential delegation of functions can lead to unclear legal liability as who is to be held responsible if the technology is inaccurate, biased, or applied unjustly.
- **Lack of transparency and accountability**- Large scale state surveillance is being deployed in the absence of any publicly available information on tendering and procurement.
- There is a lack of clarity on who is allowed to bid, the manner in which selection is made, the terms of reference around which such procurement contracts are issued, etc.
- **Drives public policy towards surveillance**- Venture-capital funded FRT companies can provide deep discounts to attract greater and more consistent clients.
- Inside an opaque system, it is unlikely that social pressure will check the efforts to proliferate the technology for surveillance.
- In the past two years, since the surge in the global conversation around FRT, several big names (Amazon, IBM, Microsoft, and most recently Meta) have claimed to impose temporary prohibition on their in-house FRT programmes.
- There are social and legal questions to be answered on the scope of participation by private enterprises, and to establish adequate checks and balances to protect constitutional and legal rights of the citizenry.

References

1. https://www.financialexpress.com/opinion/facial-recognition-technology-the-problem-with-private-play-in-frt/2393539/
2. https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html