Vetrii's
UPSC GATEWAYY
DAILY CURRENT AFFAIRS 16TH JULY 2019

WHY IS INDIA SETTING UP A MOBILE PHONE HANDSETS DATABASE?

Prelims: Governance- Institutional Reforms, Science & Technology- Information Technology

Prelims Tag: CEIR, IMEI Database, National Telecom Policy

Mains: GS-II- Government policies and interventions for development in various sectors and issues arising out of their design and implementation.

GS-III- Awareness in the fields of IT, Space, Computers, robotics, nano-technology, bio-technology and issues relating to intellectual property rights.

Mains Tag: IMEI Database, CEIR, Information security.

- **Context:** The National Telecom Policy of 2012 calls for the establishment of a National Mobile Property Registry to address the issue of "security, theft, and other concerns including reprogramming of mobile handsets".
- Based on this, the Department of Telecommunications (DoT) under the Ministry of Communications initiated a Central Equipment Identity Register (CEIR) for mobile service providers. The DoT issued a memorandum in July 2017 announcing the CEIR with a pilot project led by Bharat Sanchar Nigam Limited in Maharashtra. In January 2018, this project was handed over to the Centre for Development of Telematics (CDoT). Now, it is all set to roll out.

What is CEIR?

- Based on a 2008 order from the DoT, every mobile network provider in India has an Equipment Identity Register (EIR), or a database of the phones connected to its network. These EIRs will now share information with a single central database, the CEIR.
- In essence, it will be a repository of information on all mobile phones connected to networks across India.
- There were over 1,026 million active wireless phone connections by the end of 2018, according to the Telecom Regulatory Authority of India.
- As per the DoT's 2017 memorandum, the CEIR will have information on the device's International Mobile Equipment Identity (IMEI) number (every phone or mobile broadband device has this unique 15 digit code that precisely identifies the device), model, version, and "other information".

- It will also know if the phone is blacklisted, and the reason why it has been blacklisted.
- Phones are identified based on the IMEI number, which you can find under the battery in many mobiles or by dialling '*#06#' on the device. Mobile phone manufacturers assign IMEI numbers to each device based on ranges allotted to them by the Global System for Mobile Communications Association. Dual SIM phones will have two IMEI numbers.

What is the purpose of a CEIR?

- Such centralised databases are meant to identify and block stolen or illegal mobile phones across networks.
- Currently, when a customer reports a mobile phone as missing or stolen, mobile service providers have the ability to blacklist the phone's IMEI in their EIRs and block it from accessing their network.
- But if the SIM is changed to a new network, it can continue to be in use. With a CEIR, all network operators will be aware that the phone is blacklisted.
- The CEIR will also access the GSMA's database of IMEI numbers to check whether the phone is authentic.
- There are cases of phones being in use with duplicate IMEI numbers, or with all zeroes instead of an authentic IMEI number.
- Most importantly, as per the DoT's 2017 memorandum, the CEIR will be able to block services to subscribers. This ability had rested with individual networks till now. The memorandum also mentions enabling "IMEI-based lawful interception", which means allowing legal authorities to use CEIR data.

What are the issues with having a CEIR?

- In its 2010 consultation paper on "issues relating to blocking of IMEI for lost/stolen mobile handsets," the Telecom Regulatory Authority of India (TRAI) raises a key issue with the CEIR — who should maintain such a high-value database? Should it be the service provider, or a neutral third party?
- In their responses to the consultation paper, many major service providers preferred having a third party, ranging from international bodies to TRAI itself as suggested by the BSNL.
- The CDoT, which is reportedly readying to roll out the service, is an autonomous entity under the DoT.
- Another major issue is cloning, or reprogramming stolen or unauthorised mobile phones to attach existing genuine IMEI numbers. Blocking cloned IMEI numbers could result in the authentic ones also being blocked.
- While the actual numbers on phones in circulation with cloned or inauthentic IMEIs are hard to pin down, Parliament, in 2012, was informed of two cases of 18,000 phones using

the same IMEI number. In 2015, the government banned the import of mobile phones with fake IMEI numbers. In 2017, the DoT framed the “prevention of tampering of the Mobile Device Equipment Identification Number, Rules, 2017” that makes it punishable to tamper with the IMEI number of a device or knowingly use such a device. However, tools to reprogramme phones remain available online, and cases of such activities are reported frequently.

- On this issue, the DoT memorandum of 2017 says the IMEI Cloning and Duplication Restriction (ICDR) software is to be integrated in the CEIR.