Mains Practice Question

End-to-end encryption (E2EE) is a secure line of communication that blocks third-party users from accessing transferred data. When the data is being transferred online, only the sender and recipient can decrypt it with a key. In that way, E2EE can help mitigate risk and protect sensitive information by blocking third parties from accessing user data when data is transferred from one source to another. This can be seen as a concern in many cases where privacy is very important, such as persons living under repressive governments, whistle-blowing, mass surveillance, businesses whose reputation depends on its ability to protect third party data.

Facebook and WhatsApp along with other social networking sites are announcing the end to end encryption to protect the privacy of people. But the National Society for the Prevention to Cruelty to Children, the UK along with other organizations have expressed significant concerns over this. According to these organizations, E2EE will reduce child safety online as it will prevent the monitoring of content that is not safe for children and might lead to child grooming and the proliferation of pornographic materials.

a. Identify the ethical issues involved in the case.
b. Suggest measures to resolve them. (250 words)

28 Feb, 2020   GS Paper 4 Case Studies

Approach

- Introduce the importance of data privacy and ethical issues arising out of it.
- Identify Stakeholders, their interests and ethical issues/dilemmas they face in such cases.
- List some other issues due to use of E2EE technology and some measure to overcome them.

Data Privacy vs Need for maintaining law and order debate has entail such scenarios where privacy could spill over into secret illegal activities creating menace to society at large like the case of proliferation of child pornography. This presents an ethical dilemma for different stakeholders in using such a technology, especially under Digital and 4th Industrial Revolution where online social networking is being increasingly used.

Stakeholder	Interest	Ethical Dilemma
Service Providers like Facebook	Earn profit by fulfilling customer's satisfaction like privacy concerns	Need to increase efficiency and output of the organisation Vs Adhering to Laws, maintain social harmony
Governments, Law Makers	Serve the cause of citizens, uphold rule of law, security	Need to allow newer technologies for economic advantage, respect people's rights Vs Remain vigilant to threats like online crimes and curtail them
Civil Society including NGOs	Analysing the impact of various regulations and technologies on public	Persuade governments and service providers for their cause
Common Citizen	Use technology for learning, communicating etc.	Attitude towards doing things in secrecy i.e. mass surveillance Vs

		Honesty, Integrity in using technology

Other Issues due to use of End-to-End Encryption technology

- Such secrecy could allow for safe communication networks to terrorist, money laundering activities.
- Security Agencies would not be able to perceive threats like the possibility of Lone Wolf Attacks, Radicalisation, Banking Frauds by monitoring such networks, as due to E2EE, messages could only be opened by sender and receiver.
- This would entail that service providers like Facebook could be relenting themselves from their social responsibility of co-operating with security agencies in tackling the cybercrime.

Measures

- E2EE could be used for small group chats, while for large scale data transmission, especially those occurring across the border, it would be better to use an alternative system that takes into account these issues. This will enable the safety of data along with privacy and also enable law enforcement agencies to monitor with proper means.
- Laws also need to be formulated that can ensure that the responsibility of service providers is not withered away by a simple change in technology. It needs to be ensured that technology is used as a tool for mass surveillance for political means, and integrity of data and privacy is maintained whilst using such technology, for example recommendations of Srikrishna Committee on Data Protection can be implemented.

PDF Refernece URL: https://www.drishtiias.com/mains-practice-question/question-555/pnt