2. British' Online Safety Bill

Why in News?

- WhatsApp's head has recently said that WhatsApp would not comply with the country's proposed Online Safety Bill (OSB) which will in effect outlaw End-to-End (E2E) encryption.

Highlights

- The OSB is a proposed British legislation aimed at improving online safety by placing "Duty of Care" obligations on online platforms.
- Clause 110 of the OSB empowers the regulator to issue notices to most internet service providers, including private messaging apps, to identify and take down Terrorismand Child Sex Exploitation and Abuse (CSEA) content.
- The OSB does not mandate removal of E2E encryption, but it would require messaging apps to scan all messages to flag such content, which would de facto mean breaking encryption.
- Privacy and free speech advocates view the OSB as a disproportionate step that allows for bulk interception and surveillance.
- Through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Indian government made it mandatory for messaging platforms with more than five million users in India to "enable the identification of the first originator" of a message, or what is commonly called traceability.
- This is not the same as asking for scanning and flagging of all encrypted content; it is about getting to the first person who sent a message that may have been forwarded multiple times.
- In India, WhatsApp did not threaten to leave the market. It instead sued the Indian government over the traceability requirement.
- This is mainly because India, with 487.5 million WhatsApp users, is home to 22% of the platform's 2.24 billion monthly active users. WhatsApp's penetration rate in India is over 97% while in the U.K., it is at about 75%.
- E2E encryption is a secure communication mechanism that allows data to be encrypted on the sender's device, transmitted securely over the internet or any communication channel, and then decrypted only by the intended recipient.

- The message can only be decrypted by the intended recipient using a unique decryption key that is only accessible by the recipient's device.
- This means that no one else, not even the service provider, can access the content of the message or data being transmitted.
- E2E encryption is used to ensure privacy and security in various communication platforms, such as messaging apps, email services, and file-sharing services, as it provides a high level of protection against unauthorized access, interception, or eavesdropping by hackers, governments, or service providers.