British’ Online Safety Bill and End-to End Encryption

Prelims: End-to End Encryption, Information Technology Rules, 2021, Information Technology Act of 2000.

Mains: British’ Online Safety Bill and End-to End Encryption.

Why in News?

Recently, WhatsApp’s head 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.**

What is the British’ Online Safety Bill?

- 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 i**ssue 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.**

Is there any Similar Law in India?

- 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%.

What is End-to-End Encryption?

- 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.

What is the other Legal Framework for Encryption in India?

- **Minimum Encryption Standards:**
  - India does not have a specific encryption law. Although, a number of industry rules, such as those governing the banking, finance, and telecommunications industries, include requirements for minimum **encryption standards to be utilised in protecting transactions.**
- **Prohibition on Encryption Technologies:**
  - Users are not authorised to employ encryption standards larger than 40 bits using symmetric key algorithms or similar methods without prior clearance and deposition of decryption keys, **according to the licensing agreement between the ISP (Internet Service Provider) and the DoT (Department of Telecommunications).**
  - There are a variety of additional rules and recommendations that use a greater encryption level than 40 bits for particular sectors.
- **Information Technology Act of 2000:**
  - It regulates electronic and wireless modes of communication, is devoid of any substantive provision or policy on encryption.

UPSC Civil Services Examination, Previous Year Question

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: D

- According to section 70B of the Information Technology Act, 2000 (IT Act), the Union Government by notification should appoint an agency named Indian Computer Emergency Response Team (CERTIn) to serve as the national agency for incident response.
- The Union Government under section 70B of the IT Act, 2000 established and notified rules of CERT-In in 2014. According to Rule 12(1)(a), it is mandatory for service providers, intermediaries, data centers and corporate bodies to report cyber security incidences to CERT-In within a reasonable time of occurrence of the incident. **Hence, 1, 2 and 3 are correct.**
- **Therefore, option D is the correct answer.**

Source: TH