End-to-End Encryption

Prelims: Cryptographic keys, Data Protection, Data Protection Laws.

Mains: Advantages and Disadvantages of End-to-End Encryption.

Why in News?

Recently, Apple has announced it will be increasing the number of data points protected by **End-to-End Encryption (E2EE)** on iCloud from 14 to 23 categories.

What is the Purpose of Announcing this?

- According to a data-breach-research by Apple, the total number of data breaches **more than tripled between 2013 and 2021.** Data of 1.1 billion personal records were exposed in 2021 alone.
- With end-to-end encryption, user data will be **protected even in case data is breached in the cloud.** The extra layer of protection would be **valuable to targets of hacking attacks launched by well-funded groups.**

What is End-to-End Encryption?

- **About:**
  - End-to-end encryption is a **communication process that encrypts data being shared between two devices.**
  - It prevents third parties **like cloud service providers, internet service providers (ISPs) and cybercriminals from accessing data** while it is being transferred.
- **Mechanism:**
  - The cryptographic keys **used to encrypt and decrypt the messages** are stored on the endpoints.
  - The process of end-to-end encryption uses **an algorithm that transforms standard text into an unreadable format.**
  - This format can only be unscrambled and read by those **with the decryption keys, which are only stored on endpoints and not with any third parties** including companies providing the service.
- **Usage:**
  - E2EE has long been used when **transferring business documents,** financial details, legal proceedings, and personal conversations.
  - It can also be used to control **users' authorisation when accessing stored data.**
  - End-to-end encryption is used to **secure communications.**
  - It is also used **to secure passwords, protect stored data and safeguard data on cloud storage.**

What are the Advantages of E2EE?

- **Security in Transit:**
  - End-to-end encryption uses public key cryptography, which stores private keys on the endpoint devices. Messages can only be decrypted using these keys, so **only people with access to the endpoint devices are able to read the message.**
- **Safety from Third Parties:**
  - E2EE ensures that user **data is protected from unwarranted parties** including service providers, cloud storage providers, and companies that handle encrypted data.
- **Tamper-Proof:**
  - With E2EE, the decryption key does not have to be transmitted; the recipient will already have it.
  - If a message encrypted with **a public key gets altered or tampered within transit,** the recipient will not be able to decrypt it, so the **tampered contents will not be viewable.**
- **Compliance**:
  - Many industries are bound by regulatory compliance laws that require **encryption-level data security.**
  - E2EE can help **organizations protect that data** by making it unreadable.

What are the Disadvantages of E2EE?

- **Complexity in Defining the Endpoints:**
  - Some E2EE implementations **allow the encrypted data to be encrypted and re-encrypted at certain points** during transmission.
  - This makes it important to clearly **define and distinguish the endpoints** of the communication circuit. **If endpoints are compromised, encrypted data may be revealed.**
- **Too Much Privacy:**
  - Government and law enforcement agencies **express concern that E2EE can protect people sharing illicit content** because service providers are unable to provide law enforcement with access to the content.
- **No Protection to Metadata:**
  - Although messages in transit are encrypted and impossible to read, information about the message - **date of sending message and recipient, for instance - is still visible,** which may provide useful information to an interloper.

What is the 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 licencing agreement between the ISP and the DoT.
  - There are a variety of additional rules and recommendations **that use a greater encryption level than 40 bits for particular sectors.**
- **The** Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:
  - It superseded the earlier Information Technology (Intermediary Guidelines) Rules 2011.
  - The new set of rules have the potential to impact the end-to-end encryption techniques of social messaging applications like WhatsApp, Telegram, Signal, etc.
- **Information Technology Act of 2000:**
  - It regulates electronic and wireless modes of communication, is devoid of any substantive provision or policy on encryption.

Source: TH