What is end-to-end encryption?

December 13, 2022

In news– Recently, Apple has announced that it will be increasing the number of data points protected by end-to-end encryption on iCloud from 14 to 23 categories.

About end-to-end encryption-

- It 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**.
- 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.
- End-to-end encryption 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, which seems to be what Apple intends to do.
- It is used to **secure communications.**
- Some of the popular instant-messaging apps that use it are Signal, WhatsApp, iMessage, and Google messages.
- However, instant messaging is not the only place where user data is protected using end-to-end encryption.
- **It is also used to secure passwords, protect stored data and safeguard data on cloud storage.**
- End-to-end encryption ensures that user data is

protected from unwarranted parties including service providers, cloud storage providers, and companies that handle encrypted data.

- No one else can access this data and it remains secure even in the case of a data breach in the cloud storage.
- The data can only be accessed with access to the device passcode, password, recovery contact, or recovery key. The technology also makes it harder for service providers to share user information from their services with authorities.
- However, end-to-end encryption does not protect metadata, which includes information like when a file was created, the date when a message is sent and the endpoints between which data was shared.

Reasons for government agencies unhappy with it-

- Attempts by government agencies across the globe, in the past, to access encrypted data hosted and stored by tech companies have met with strong resistance.
- In 2019, the U. S., the U. K., and Australia planned to pressure Facebook to create a backdoor into its encrypted messaging apps.
- Australia, in 2018, passed laws that would force tech companies and service providers to build capabilities allowing law enforcement secret access to messages on platforms like WhatsApp and Facebook.