WhatsApp vs Government

Why In News

- **WhatsApp told Delhi High Court** that the instant messaging platform will exit India if it is forced **to break end-to-end encryption of messages** on its platform. This came after the **High Court received petitions** from WhatsApp and its parent company Meta.

- The petitions **challenged the 2021 Information Technology** (IT) rules that apply to social media intermediaries. According to the new rules, WhatsApp is required to trace chats and establish means to identify the first originator of information. **The Indian government announced** the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on February 25, 2021. These rules require large social media platforms like Twitter, Facebook, Instagram, and WhatsApp to comply with the latest norms.

What Is The Matter All About

- WhatsApp **filed a petition in 2021**, stating that the requirement of intermediaries enabling the identification of the first originator of information in India puts end-to-end encryption and its benefits "at risk."

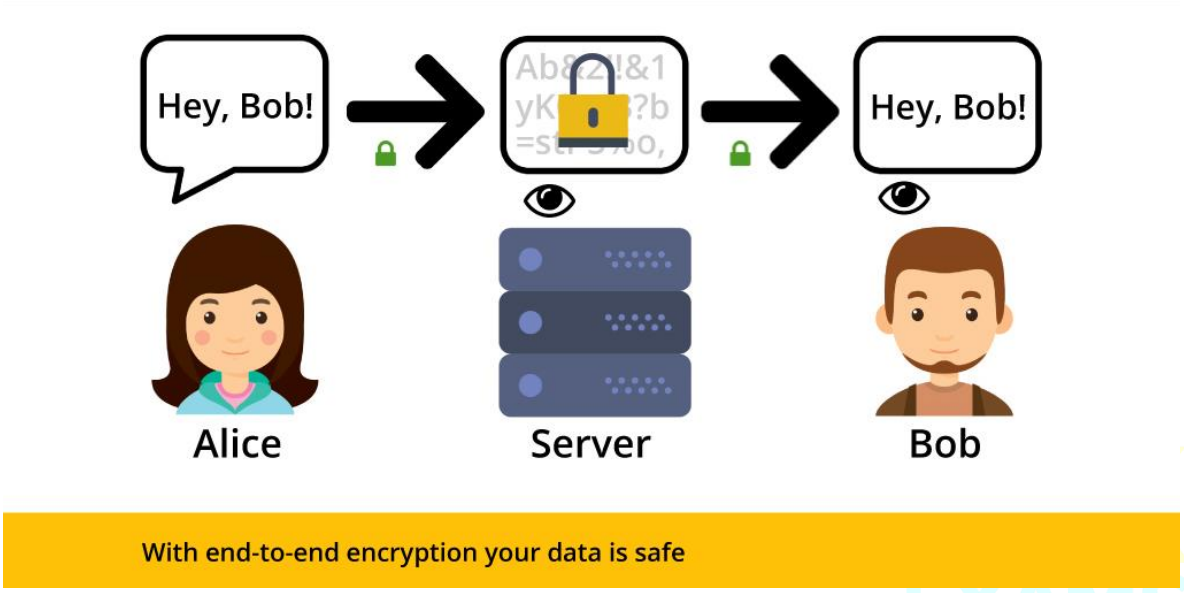
- **The traceability provision forces** the company to break end-to-end encryption on its messaging service, as well as the privacy principles underlying it. **Facebook and WhatsApp have challenged** the new rules on the grounds that they violate the right to privacy and are unconstitutional.

What Is The Government's Argument

- **Ministry of Electronics and Information Technology** (MeitY) has argued that if the **IT Rules, 2021**, are not implemented, law enforcement agencies will find it difficult to trace the **origins of fake and misleading information** that will percolate in other platforms, disturbing peace and harmony in society and leading to public order problems.

What Is end-to-end Encryption

- End-to-end encryption is a **secure method of protecting data** by encrypting it at the sender's device and decrypting it at the receiver's device. This method ensures that the data remains secure from the moment it is sent until it reaches its intended recipient. **Unlike traditional encryption methods**, end-to-end encryption does not allow any third-party to access the data, including the service provider.



- For instance, email services like Gmail, Google, or Microsoft have copies of the decryption keys, which allow them to access users' content on their servers. This access enables service providers to read users' emails and files. Google has used this possession of decryption keys to target advertisements to the Google account holder in the past.
- **End-to-end encryption protects** the message from prying eyes because only the sender and receiver have access to the decryption keys. Even if an intermediary server relays the message, it cannot be understood.
- End-to-end encryption also safeguards against fraud by preventing message tampering. Cybercriminals often attempt to alter information either out of malice or for fraudulent purposes.
- **E2EE encrypted messages** cannot be predictably changed, making it easier to detect tampering and alert users that the data is compromised.

Can WhatsApp Read Your Messages

- At the time of launch of end-to-end encryption, the **founders of WhatsApp had made** it clear that only the sender and receiver could read the messages. That is, not even WhatsApp itself could read them.
- “The idea is simple: when you send a message, the only person who can read it is the person or group chat that you send that message to,” WhatsApp founders **Jan Koum and Brian Acton** had said while announcing the feature.

- “No one can see inside that message. Not cybercriminals. Not hackers. Not oppressive regimes. Not even us. End-to-end encryption helps make communication via WhatsApp private – sort of like a face-to-face conversation,” they added.
- “Before a message ever leaves your device, it’s secured with a cryptographic lock, and only the recipient has the keys. In addition, the keys change with every single message that’s sent,” it explained.

Why end-to-end Encryption Is A Challenge For Government

- **Governments worldwide want tech companies** to implement measures that allow them to bypass end-to-end encryption (E2EE) as and when needed, on national security grounds. This has become a major point of contention between governments, tech companies, and privacy advocates.
- The **E2EE inhibits law enforcement's ability** to gather data that could lead to the protection of vulnerable individuals.

- **Protecting children from harmful online** content is a commonly cited example of when E2EE can threaten the safety of individuals. Another example is the difficulty in preventing access to, and distribution of, extremist material.

How Other Countries Deal With The Issue

- This struggle between **law enforcement agencies** and tech giants over privacy of personal data of users is an ongoing discussion. Governments and agencies across the world are looking at enforcing rules for technology companies to enable access to users' data, which may undermine the security of their devices or platforms.

- "In the **United States and the European Union**, there is growing scrutiny over encryption, driven by the need to combat serious crimes such as the spread of child sexual abuse material". "However, these regions have also shown a robust commitment to preserving individual privacy and security online," he added.
- The **US, for example, has not enforced laws** that require backdoors to be created into encrypted services, understanding that such measures could compromise the security of all users, he said.

- Similarly, **EU regulations, guided by robust data protection laws** like the General Data Protection Regulation, uphold the sanctity of encryption while balancing it with law enforcement requirements.
- Last year, in response to a legislation the **UK government was working** on, which may have compelled technology companies to break end-to-end encryption on private messaging services, representatives of leading instant messaging platforms, including Signal, Viber and WhatsApp wrote an open letter voicing their grievances.

- "**We don't think any company, government or person** should have the power to read your personal messages and we'll continue to defend encryption technology," the companies wrote in their letter.
- They added, "**We're proud to stand** with other technology companies in our industry pushing back against the misguided parts of this law that would make people in the UK and around the world less safe."

- The letter also said that, around the world, businesses, individuals and governments face persistent threats from online fraud, scams and data theft — **"Malicious actors and hostile states** routinely challenge the security of our critical infrastructure."
- Adding, **"End-to-end encryption** is one of the strongest possible defences against these threats, and as vital institutions become ever more dependent on internet technologies to conduct core operations, the stakes have never been higher."