End-to-End Encryption is an asymmetrical type of encryption that is used to transmit messages (be it text, images, videos, or any sort of data) through the web securely. Usually, End-to-End encryption relies on the message's sender to possess two keys, a Private Key and a Public Key. The sender encrypts their data using the receiver's public key and sends it unto the world, where no one can decrypt it, other than the receiver's private key.

Since companies don't wish to be involved in data leak scandals, they implement secure End to End encryption, which disallows anyone, including the company itself from viewing said data.

The issue arises when government agencies require data for what they claim to be security purposes. Personal privacy has to be sacrificed in order for criminal investigations to continue. The effect at which the provided data helps security is still debated today. What the US government want specifically is a backdoor to the security, a master key that allows them to unlock any phone, any WhatsApp account, etc.

Another issue of adding a backdoor to End to End encryption is that the backdoor can allow foreign entities to maliciously steal data from people. The issue isn't limited to personal use. It can extend to countries spying on each other.

Mohand Alrasheed 439101298