Google end-to-end encryption

Google has officially confirmed rolling out end to end encryption for messages for Android users. The company wants to make it harder for anyone including law enforcement to read the message content.  
The change is part of Google's Rich Communication Service (RCS) standard upgrade. Google is upgrading from SMS to RCS for Android users. The feature will enable additional features for images and video sharing. Since this is a global rollout, the update will be available to all people communicating using Android-powered devices.  
The move brings additional privacy and security to Google's messaging application. The update comes amid rising complaints from law enforcement agencies around strong encryption that enabled criminals to hide their tracks.  
Encryption will be available for those users who have signed up for the public beta for Android messages. The move is a big win for privacy advocates. The encryption is already available for Facebook-owned WhatsApp. The company has been facing massive resistance over its plan to bring full encryption to the Messenger app.  
While announcing the rollout, Google Product Lead, Drew Rowny said, "End-to-end encryption ensures that no one, including Google and third parties, can read the content of your messages as they travel between your phone and the phone of the person you're messaging."  
Google wants to make its encryption implementation part of the Universal Profile Standard. Apple has already put pressure on GSMA (the carrier consortium) to move towards more encryption.  
Even back in 2016, Google had offered end-to-end encryption its Allo messaging app. But the company had to kill the app as it failed to gain popularity.