Major messaging clients (Messenger, WhatsApp, Skype, iMessage, etc) use a centralized system where messages are relayed through a central server.

This central server can learn:

- Who is talking to whom
- When messages are sent
- Potentially more (when messages are read, etc)

No single entity should be able to learn metadata.

Any pair of users who are talking.

When messages are sent between users.

Messages Encrypted End to End.

Secure Login/Credentials.

No Leaks of Sensitive Information (IPs, etc)

iOS Client Application

Use of Peer-to-Peer connections

Avoids Central Server

Easy Allows End-to-End Encryption

Registration Service for Login/Discovery

Coordinates initial discovery, but doesn’t see any actual traffic