What Data the FBI can Legally Access from Secure Messaging Apps

Source: Internal FBI document, accessed in 2021 through FOIA request by Property of the People

WeChat

***No message content.**
*Accepts account preservation letters and subpoenas, but cannot provide records for accounts created in China.
*For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active.

WhatsApp

***Message content limited.**
***Subpoena:** can render basic subscriber records.
***Court order:** Subpoena return as well as information like blocked users.
***Search warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts.
***Pen register:** Sent every 15 minutes, provides source and destination for each message.
*If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content.

Wickr

***No message content.**
*Date and time account created.
*Type of device app installed on.
*Date of last use.
*Number of messages.
*Number of external IDs (email addresses and phone numbers) connected to the account, bot not to plaintext external IDs themselves.
*Avatar image.
*Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information).
*Wickr version number.

Line

***Message content limited.**
*Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.)
*Information on usage.
*Maximum of seven days worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed).

Apple iMessage

***Message content limited.**
***Subpoena:** can render basic subscriber information.
***18 USC §2703(d):** can render 25 days of iMessage lookups and from a target number.
***Pen Register:** no capability.
***Search Warrant:** can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud.

Telegram

***No message content.**
*No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP and phone number to relevant authorities.

Viber

***No message content.**
*Provides account (i.e. phone number)) registration data and IP address at time of creation.
*Message history: time, date, source number, and destination number.

Signal

***No message content.**
*Date and time a user registered.
*Last date of a user's connectivity to the service.

Threema

***No message content.**
*Hash of phone number and email address, if provided by user.
*Push Token, if push service is used.
*Public Key
*Date (no time) of Threema ID creation.
Date (no time) of last login.