<PRIVACY ASSESSMENT> MESSENGER SERVICES

A COMPARISON OF

SIGNAL

IMESSAGE

TELEGRAM

WHATSAPP

CLUBHOUSE

FACEBOOK MESSENGER

Legal Engineer
Ing. Mag. Matthias M. Hudobnik, FIP, CIPP/E, CIPT, DPO, CIS LA
http://www.hudobnik.at • matthias@hudobnik.at

INTRODUCTION

Messaging platforms (e.g., WhatsApp Messenger, Facebook Messenger, Telegram Messenger, iMessage, Signal - Private Messenger, etc.) are widely used but show great differences in terms of privacy implications and data protection. Also, the invitation-only social media app Clubhouse: Drop-in audio chat is enjoying great enthusiasm among iOS users and raises some security and privacy concerns.
The goal of this point of view is to give a brief overview of the different messaging apps for electronic communication and outline their strengths and weaknesses. Moreover, the document will outline which data is linked to the app users, focusing on the following messaging apps:

- Signal - Private Messenger
- iMessage
- Telegram Messenger
- WhatsApp Messenger
- Facebook Messenger
- Clubhouse: Drop-in audio chat

MESSAGING PLATFORMS[1]

Signal – Private Messenger[2]

The company's jurisdiction is the USA, and they are funded by the Freedom of the Press Foundation, the Knight Foundation, the Shuttleworth Foundation, the Open Technology Fund, and the Signal Foundation. The company does not collect customers' data but minimal user data (the mandatory mobile number is sent to a third party for registration and recovery purposes). The encryption function is turned on by default and the app uses Curve25519 / AES-256 / HMAC-SHA256 schemes. Personal information (e.g., mobile number, contact list, etc.) is mostly hashed and the messages cannot be read by the company. The app generates and keeps a private key on the device itself and encrypts metadata. The app uses TLS/Noise to encrypt network traffic and allows a secondary factor of authentication. The company does not log timestamps/IP addresses. Signal - Private Messenger provides self-destructing messages.[3]

The following data is linked to the app user:

App Functionality
There is no data link to the app user.

[1] Zak Doffman, Why You Should Stop Using Facebook Messenger After Privacy Backlash, available at <https://www.forbes.com/sites/zakdoffman/2021/01/16/stop-using-facebook-messenger-after-whatsapp-vs-apple-imessage-and-signal-privacy-backlash/?sh=4b263ccc4650> accessed on 09/11/2021.
[2] More information about the Signal – Private Messenger and the Signal Foundation, available at <https://signal.org> and <https://en.wikipedia.org/wiki/Signal_(software)> and <https://restoreprivacy.com/secure-encrypted-messaging-apps/signal> accessed on 09/11/2021.
[3] Secure Messaging Apps Comparison, available at <https://www.securemessagingapps.com> and <https://en.wikipedia.org/wiki/Comparison_of_cross-platform_instant_messaging_clients> accessed on 09/11/2021.

iMessage[4]

The company's jurisdiction is the USA, and they are funded by Apple. The company collects customers' data and sends user data and/or metadata to the parent company and/or third parties. The encryption function is turned on by default and the app uses RSA-1280 (encryption), ECDSA 256 (signing) / AES 128 / SHA-1 schemes. Personal information (e.g., mobile number, contact list, etc.) is not hashed and the messages cannot be read by the company. The app generates and keeps a private key on the device itself but does not encrypt metadata. The app uses TLS/Noise to encrypt network traffic and does not allow a secondary factor of authentication. The company logs timestamps/IP addresses. iMessage does not provide self-destructing messages.[5]

The following data is linked to the app user:

App Functionality
Contact Information -E-Mail Address -Phone Number
Search History
Identifiers -Device ID

Telegram Messenger[6]

The company's jurisdictions are USA, UK, Belize, UAE, and they are funded by Pavel Durov. The company does not collect customers' data but sends user data and/or metadata to the parent company and/or third parties. The encryption function is turned off by default and the app uses Curve25519 256 / XSalsa20 256 / Poly1305-AES 128 schemes. Personal information (e.g., mobile number, contact list, etc.) is not hashed and the messages can be read by the company. The app generates and keeps a private key on the device itself but does not encrypt metadata. The app does not use TLS/Noise to encrypt network traffic but allows a secondary factor of authentication. The company logs timestamps/IP addresses. Telegram Messenger provides self-destructing messages.[7]

The following data is linked to the app user:

App Functionality
Contact Information -Name -Phone Number
Contacts
Identifiers -User ID

[4] More information about iMessage and Apple, available at <http://support.apple.com/explore/messages> and <https://en.wikipedia.org/wiki/IMessage> accessed on 09/11/2021. See also Zak Doffman, Why Apple's New iMessage Security Update Beats WhatsApp On Your Phone, available at <https://www.forbes.com/sites/zakdoffman/2021/02/06/whatsapp-beaten-by-new-imessage-update-for-apple-iphone-users/?sh=76c43f585698> accessed on 09/11/2021.

[5] See Fn. 3.

[6] More information about Telegram Messenger, available at <https://telegram.org> and <https://en.wikipedia.org/wiki/Telegram_(software)> and <https://restoreprivacy.com/secure-encrypted-messaging-apps/telegram> accessed on 09/11/2021.

[7] See Fn. 3.

WhatsApp Messenger[8]

The company's jurisdiction is the USA, and they are funded by Facebook. The company collects customers' data and sends user data and/or metadata to the parent company and/or third parties. The encryption function is turned on by default and the app uses Curve25519 / AES-256 / HMAC-SHA256 schemes. Personal information (e.g., mobile number, contact list, etc.) is not hashed and the messages cannot be read by the company. The app generates and keeps a private key on the device itself but does not encrypt metadata. The app uses TLS/Noise to encrypt network traffic and allows a secondary factor of authentication. The company logs timestamps/IP addresses. WhatsApp Messenger provides self-destructing messages.[9]

The following data is linked to the app user:

App Functionality	Analytics
Contact Information -E-Mail Address -Phone Number	*Purchases* -Purchase History
Purchases -Purchase History	*Location* -Coarse Location
Financial Information -Payment Information	*Contact Information* -Phone Number
Location -Coarse Location	*User Content* -Other User Content
Contacts	*Identifiers* -User ID -Device ID
User Content -Customer Support -Other User Content	*Usage Data* -Product Integration -Advertising Data
Identifiers -User ID -Device ID	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data
Usage Data -Product Interaction	
Diagnostics -Crash Data -Performance Data -Other Diagnostic Data	

Facebook Messenger[10]

The company's jurisdiction is the USA, and they are funded by Facebook. The company collects customers' data and sends user data and/or metadata to the parent company and/or third parties. The encryption function is turned off by default and the app uses Curve25519 / AES-256 / HMAC-SHA256 schemes. Personal information (e.g., mobile number, contact list, etc.) is not hashed and the messages can be read by the company. The app generates and keeps a private key on the device itself but does not

[8] More information about WhatsApp Messenger, available at <https://www.whatsapp.com> and <https://en.wikipedia.org/wiki/WhatsApp> accessed on 09/11/2021.

[9] See Fn. 3.

[10] More information about Facebook Messenger, available at <https://www.messenger.com> and <https://en.wikipedia.org/wiki/Facebook_Messenger> and <https://www.forbes.com/sites/zakdoffman/2021/02/02/whatsapp-just-gave-you-a-reason-to-stop-using-facebook-messenger-after-imessage-privacy-backlash/?sh=38ad4f474673> accessed on 09/11/2021.

encrypt metadata. The app uses TLS/Noise to encrypt network traffic but does not allow a secondary factor of authentication. The company logs timestamps/IP addresses. Facebook Messenger provides self-destructing messages.[11]

The following data is linked to the app user:

App Functionality	**Analytics**	**Third-Party Advertising**	**Product Personalization**	**App Functionality**	**Other Purposes**
Health & Fitness	*Purchases* -Purchase History	*Purchases* -Purchase History	*Purchases* -Purchase History	*Health & Fitness*	*Purchases* -Purchase History
Purchases -Purchase History	*Location* -Coarse Location -Precise Location	*Financial Information* -Other Financial Information	*Financial Information* -Other Financial Information	*Purchases* -Purchase History	*Financial Information* -Other Financial Information
Financial Information -Payment Information -Credit Information -Other Financial Information	*Contact Information* -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information	*Location* -Precise Location -Coarse Location	*Location* -Precise Location -Coarse Location	*Financial Information* -Other Financial Information	*Location* -Precise Location -Coarse Location
Location -Coarse Location -Precise Location	*User Content* -Photos or Videos -Audio Data -Gameplay Content -Customer Support -Other User Content	*Contact Information* -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information	*Contact Information* -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information	*Location* -Precise Location -Coarse Location	*Contact Information* -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information
Contact Information -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information	*Identifiers* -User ID -Device ID	*Contacts*	*Contacts*	*Contact Information* -Physical Address -E-Mail Address -Name -Phone Number -Other User Contact Information	*Contacts*
Contacts	*Health & Fitness*	*User Content* -Photos or Videos -Gameplay Content	*User Content* -Photos or Videos -Gameplay Content	*Contacts*	*User Content* -Photos or Videos -Gameplay Content

[11] See Fn. 3.

		-Other User Content	-Other User Content		-Customer Support -Other User Content
User Content -E-Mails or Text Messages -Photos or Videos -Audio Data -Gameplay Content -Customer Support -Other User Content	*Usage Data* -Product Integration -Advertising Data -Other Usage Data	*Search History*	*Search History*	*User Content* -E-Mails or Text Messages -Photos or Videos -Audio Data -Gameplay Content -Customer Support -Other User Content	*Search History*
Search History	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data	*Browsing History*	*Browsing History*	*Search History*	*Browsing History*
Browsing History	*Financial Information* -Payment Information -Other Financial Information	*Identifiers* -User ID -Device ID	Identifiers -User ID -Device ID	*Browsing History*	*Identifiers* -User ID -Device ID
Identifiers -User ID -Device ID	*Contacts*	*Usage Data* -Product Interaction -Advertising Data -Other Usage Data	*Usage Data* -Product Interaction -Advertising Data -Other Usage Data	*Identifiers* -User ID -Device ID	*Usage Data* -Product Interaction -Advertising Data -Other Usage Data
Usage Data -Product Interaction -Advertising Data -Other Usage Data	*Search History*	*Other Data* -Other Data Types	*Sensitive Information*	*Usage Data* -Product Interaction -Advertising Data -Other Usage Data	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data
Sensitive Information	*Browsing History*	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data	*Sensitive Information*	*Other Data* -Other Data Types
Diagnostics -Crash Data -Performance Data -Other Diagnostic Data	*Sensitive Information*		*Other Data* -Other Data Types	*Diagnostics* -Crash Data -Performance Data -Other Diagnostic Data	
Other Data -Other Data Types	*Other Data* -Other Data Types			*Other Data* -Other Data Types	

Clubhouse: Drop-in audio chat[12]

The concept of this social network app is based on the principle of landing by a user who already uses the app. The purpose of the app is to host virtual live discussions where users can engage in audio-based conversations through speaking or listening to different discussions. The company's jurisdiction is the USA, and they are funded by Alpha Exploration. The Stanford Internet Observatory analyzed the app and clarified that Clubhouse is using a software development kit (SDK) established by the Chinese company Agora and implicated a theoretical access request of personal data through Chinese intelligence laws.[13]

The app temporally records live audio sessions in case of investigating an incident, but records will be deleted after the investigation is finished otherwise the respective data will be deleted after the live session. The audio recordings are encrypted. If app users upload, synchronize, or import data, it will be used to improve the service and the user experience. According to the company's privacy policy, they may collect shared user content (e.g., types of conversations, interactions with others, features used, time, frequency, and duration of usage).[14]

Worth mentioning is the fact that the Clubhouse app allows anyone to carry out mass scrapes of user data. The architecture of the app allows this through the application programming interface (API) or a token, where anyone can interrogate the complete body of public Clubhouse user profile information. This security vulnerability was revealed by a data leak of 1.3 million scraped user records published on the Internet.[15]

The breach or hack has been denied by Clubhouse and it has been made clear that the revealed data elements were public profile information that can be accessed by anyone via their API.[16]

According to the company's privacy policy, there are also compliance issues with the GDPR in terms of their service and data transfers to the USA as well as sharing user data with third parties since the company resides in the USA.[17]

The following data is linked to the app user (the list is not conclusive):

App Functionality
Contact Information -Name -Phone Number -E-Mail Address
Identifiers -User ID

[12] More information about Clubhouse: Drop-in audio chat, available at <https://www.joinclubhouse.com> and <https://en.wikipedia.org/wiki/Clubhouse_(app)> accessed on 09/11/2021.

[13] See Jack Cable, Matt DeButts, Renee DiResta, Riana Pfefferkorn, Alex Stamos, David Thiel, Stanford Internet Observatory, Clubhouse in China: Is the data safe?, available at <https://cyber.fsi.stanford.edu/io/news/clubhouse-china#appendix> accessed on 09/11/2021. See also Stiftung Warentest, Gehypte Chat-App plaudert Nutzer-daten aus, available at <https://www.test.de/Clubhouse-im-Datenschutz-Check-Gehypte-Chat-App-plaudert-Nutzerdaten-aus-5713421-0> accessed on 09/11/2021. See also Cornelia Möhring, Heise Online, Clubhouse-FAQ - alles, was Sie zur neuen App wissen müssen, available at <https://www.heise.de/tipps-tricks/Clubhouse-FAQ-alles-was-Sie-zur-neuen-App-wissen-muessen-5030451.html> accessed on 09/11/2021.

[14] See Privacy Policy, Alpha Exploration, available at <https://www.notion.so/Terms-of-Service-cfbd1824d4704e1fa4a83f0312b8cf88> accessed on 09/11/2021.

[15] See Cybernews, Clubhouse data leak: 1.3 million scraped user records leaked online for free, available at <https://cybernews.com/security/clubhouse-data-leak-1-3-million-user-records-leaked-for-free-online> accessed on 09/11/2021. See also Katie Canales, Scraped personal data of 1.3 million Clubhouse users has reportedly been posted online, available at <https://www.businessinsider.com/clubhouse-data-leak-1-million-users-2021-4?r=DE&IR=T> accessed on 09/11/2021.

[16] See Clubhouse official Twitter page, available at <https://twitter.com/joinClubhouse/status/1381066324105854977?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1381066324105854977%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcybernews.com%2Fsecurity%2Fclubhouse-data-leak-1-3-million-user-records-leaked-for-free-online%2F> accessed on 09/11/2021.

[17] See Stefan Hessel, reuschlaw, "Clubhouse": can companies use the app while adhering to the GDPR?, available at https://www.reuschlaw.de/en/news/clubhouse-can-companies-use-the-app-while-adhering-to-the-gdpr> accessed on 09/11/2021.

-Mobile Phone Type -Mobile Operator
Usage Data -Chatroom ID -Chat Room Interactions -Information about People, Accounts, and Clubs
User Content -Photos -Audio Data Chatroom
Time -Chat Room Interactions -App Interaction in total

CONCLUSION

The architecture of Signal - Private Messenger follows the data protection principles of data minimization, privacy by design, and privacy by default. The app only processes the necessary personal data to provide the service to its users. A disadvantage is that the app cannot be used without registration via your mobile number.

Concerning WhatsApp Messenger, an advantage is the ease of use and the wide distribution. However, there is a risk that backups (that are not end-to-end encrypted) will be sent to the cloud if not configured carefully. Other disadvantages are WhatsApp's affiliation with Facebook and the associated data exchange.

With regards to Facebook Messenger, end-to-end encryption can only be used at the expense of usability. However, without enabled encryption, data protection and privacy are not guaranteed.

Telegram Messenger developed encryption algorithms, MTProto (a custom protocol) but end-to-end encryption is only maintained for secret chats and the use of their service requires registration via mobile number too. Telegram Messenger also logs IP addresses and other user data.

iMessage has one of the best architectures, supporting the synchronization of messages across multiple devices while preserving end-to-end encryption. A big disadvantage is that its service doesn’t work cross-platform because it is only for Apple users.

Concerning Clubhouse: Drop-in audio chat, there are various security and data protection issues in the architecture of the app that cannot be denied. It remains to be seen how the company will react to any suggestions for improvement and notices from data protection authorities despite their hype in terms of usage. In any case, every user should be aware of the possible risks associated when using this app.

Finally, it may be advisable to use different messaging apps in parallel to prevent data aggregation, but it always depends heavily on the circumstances and business case to choose the most appropriate messaging app.