TeleMessage

Comparing Chat Applications Encryption and Safe Usage

Table of Contents

03 Executive Summary

05 How Private and Transparent is Your Mobile Chat Application?

09 The Information Stored by Mobile Messaging Applications About Their Users

11 Possibilities of Data Leakage in Mobile IM Applications

14 Best Practices to Follow While Using a Mobile Messaging Application

17 About TeleMessage

20 Resources

Executive Summary

Human beings have come a long way, from making gestures, to sending messages with the tap of a button, to communicating with fellow beings. Communication has become seamless and intuitive with powerful capabilities accessible for all users.

Technological progress has helped communication advance from its infant stage. Today, phone calls and video calls allow people to communicate with each other, no matter how far they are in this world. With emails, text messages, and mobile chats, the need for oral communication has further reduced. Mobile chat applications like WhatsApp and WeChat not only let you send texts, multimedia, and files, but also allow you to send emoticons and stickers (picture messages), create groups, and get read and deliver confirmations. Features like these help people to express their thoughts as succinctly as if they were having a live face-to-face conversation.

The use of mobile messaging applications continues to increase. Whether for business or personal use, mobile IM (Instant Messaging) applications offer a level of simplicity that cannot be compared to any other method of communication. Mobile IM applications like WhatsApp, FB Messenger, Telegram, WeChat, and Signal are the current trendsetters in the communication market. Despite the fact that all these applications do not have the same features, they are very similar in their basic nature of the operation, offering: chats, voice calls, and video calls. But irrespective of the offered features, all users will require ‘privacy’, with a discretionary setting for how much information to reveal your information to strangers.

Have you ever wondered how private your conversations are with your friends and family? Are you sure that the messages and sensitive information you share over mobile IM applications are being seen only by you and your texting counterpart? Let us dive deeper and compare the security setting in different messaging apps.

This whitepaper provides:

- An overview of the privacy and transparency that users get while using a mobile chat application
- Checking the possibilities of personal information getting compromised while using mobile messaging apps
- An overview of the user information stored by different mobile messaging applications
- Best practices that a user should follow, while using a mobile IM application

How Private and Transparent is Your Mobile Chat Application?

End-to-end encryption is considered the gold standard with respect to data privacy in mobile chat applications. It is the practice of encrypting a message at the time of transmission and decrypting it on the recipient's device. The advantage of using this feature is that only the sender and recipient will be able to see the messages, and no one will be able to intercept them while they are in transit. Therefore, users can rest assured that their chats are not being monitored by some stranger. People have become increasingly concerned about privacy, so most mobile messaging applications have adopted this security feature to provide data security to their users. In this manner, trust between the users and the service providers will increase.

The Facebook-owned WhatsApp is the most popular and most used mobile chat application, with all WhatsApp messages end-to-end encrypted by default, neither a third-party nor the service operator can access your messages in WhatsApp. But the company does not encrypt the metadata of your conversations, rendering it visible to WhatsApp. WhatsApp also collects specific user information and its application code is not available for public review. Finally, WhatsApp releases a transparency report outlining what kinds of data they gather from you.

Messenger is another Facebook-owned mobile messaging application that also uses end-to-end encryption. But unlike WhatsApp, conversations in Messenger are not end-to-end encrypted by default. You will have to turn on **Secret Conversations** to send end-to-end encrypted messages. Messenger also does not encrypt metadata of your conversations, which means Facebook can view it. In addition to this, Facebook collects user information from Messenger. Like WhatsApp, Messenger also releases a transparency report that shows the details acquired from its users, and its application code is not open to the public.

Telegram, owned by Pavel Durov, has its origins in Russia. Telegram also provides end-to-end encryption for the messages sent and received through the application. But this feature is not turned on by default for all your conversations. If you wish to have an encrypted chat, you will have to turn on the **Start Secret Chat** option in the profile you wish to use. The metadata of your conversations is not encrypted, either. Telegram only collects basic app information from its users. The company does not release a transparency report, but the application code is open to the public. However, their application code for the server is not available for public scrutiny.

Tencent-owned WeChat is China's version of WhatsApp. The application isn't popular outside the walls of China (at least not as popular as WhatsApp or Telegram), yet no other application can compete with its reach inside China. But due to the strict regulations imposed by the Chinese government, the company can only do so much in providing privacy for the user's conversations through the application. Neither the WeChat conversations nor their metadata are end-to-end encrypted. For this reason, your WeChat conversations can be monitored by the company if they choose to do so. WeChat also collects user information. But it is unknown to what extent, as the company does not release a transparency report. WeChat also does not share its application code with the public.

If you are eager to choose a winner for the most private chat application out of the four mentioned above, then you might want to wait for the next one.

Signal is a relatively young mobile IM chat application compared to its competitors, and it is run by the Signal Technology Foundation. Signal's primary concern is the privacy of its users, and for this reason, its security and transparency are unrivaled in comparison to its competitors. Signal offers end-to-end encryption by default on all conversations sent and received through it. Since the metadata of the conversation is also encrypted, there is very little chance of your conversations being leaked. Since Signal is run by a non-profit organization and relies on donations, it does not attempt to collect user data.

Furthermore, by releasing a transparency report and making their application code available to the public, Signal offers better transparency for their engagement with users.

So that makes Signal the winner? Although Signal offers greater privacy and transparency than the other mobile chat applications that we discussed above, all other applications offer user privacy in their own way. Hence, it is safe to assume that all these applications are relatively safe to use, provided we, the users are aware of how to use them.

The Information Stored by Mobile Messaging Applications About Their Users

Most people don't bother to read the details on the screen when installing a chat application. It is always a good idea to read the application's terms of use so that you are aware of what information the application collects from you. Let us review the type of information that each mobile messaging application collects from its users.

Information that each application stores about its users

	Contact Details	End-to-end Encryption	Personal Information	Information about mobile device	Location Data	Ad Sells	Availability, Conversation Length, Interactions Network, Groups Data
WHATSAPP	✓	✓	✓	✓	✓	✓	✓
MESSENGER	✓	✓	✓	✓	✓	✓	✓
TELEGRAM	✓	✓	✗	✓	✓	✓	✓
SIGNAL	✗	✓	✗	✗	✗	✗	✗
WECHAT	✓	✓	✓	✓	✓	✓	✓

Note: Even with all the above privacy limitations, all these apps are considered safe and secure to use.

Even though all these mobile messaging applications seem to be the same in terms of their usage, there are some differences in their offerings. While some mobile chat applications offer end-to-end encryption for their messages by default, some others provide this feature as an option, where the user has to turn this feature on, manually. Certain other applications don't offer end-to-end encryption at all.

TeleMessage has summarized the differences between popular mobile chat applications. The table given below gives readers an idea about how these messaging tools differ from each other.

TeleMessage summarized the differences between different popular messaging tools

	Is information sent in an encrypted manner) end-to-end)?	Is information encrypted in a way that the service operator cannot access?	Is metadata (about communication) encrypted?	Does the company refrains from collecting information from users?	Is the application code open to the public?	Does the company disclose/release a transparency report?
WHATSAPP	✓	✓	✗	✗	✗	✓
MESSENGER	✓	✗ (but There is an option for encrypted chats)	✗	✗	✗	✓
TELEGRAM	✓	✗ (but There is an option for encrypted chats)	✗	Partial, Data encrypted on servers, only basic app information collected	App ✓ Server ✗	✗
SIGNAL	✓	✓	✓	✓	✓	✓
WECHAT	✗	✗	✗	✗	✗	✗

It is evident from the tables given above that even though the basic idea of all the mobile messaging applications remains the same, the features and mode of operation of each application are unique. Hence, recording and archiving the conversations through these applications is very essential to meet regulatory compliance, while using the applications for business communication.

Possibilities of Data Leakage in Mobile IM Applications

While WhatsApp is still the most preferred mobile messaging application in the world, there is no other application that can dominate the reach of WeChat in China. Applications like Telegram and Signal are also gaining popularity these days.

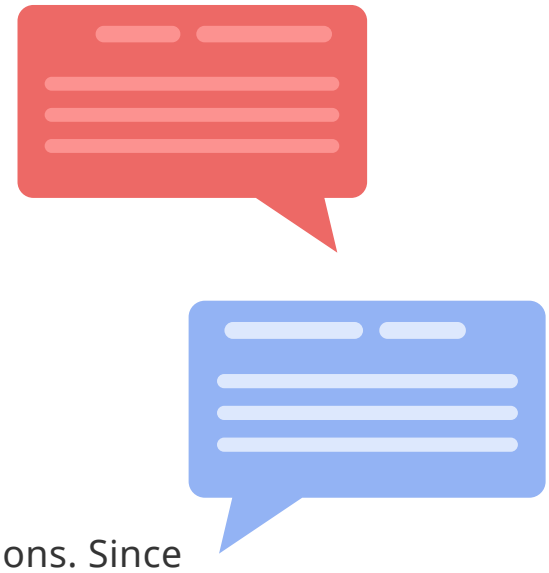
Conversations in these mobile chat applications may range from as simple as the recipe of a pancake, to as complex as the decisions involving a stock trade, or even more. Hence, the level of security and privacy that the users demand from these applications is very high. And most of the IM applications in the market do think about their users' privacy and security while designing the applications. Services like end-to-end encryption, two-factor authentication, manual, as well as auto-deletion of sent messages, are all part of the concerns revolving around the user's privacy and security.

While mobile messaging apps continue to provide their users with new features to enhance the user's security and privacy, there are individuals or organizations that are on the constant lookout for vulnerabilities in these chat applications. The recent events that involve a "high" severity rating advisory issued by CERT-In for WhatsApp users, and the successful access to Signal by a digital investigation tool points to the fact that users must be vigilant while using mobile IM applications.

The CERT-In or the Indian Computer Emergency Response Team is the national nodal agency of India for responding to computer security incidents as and when they occur. The agency has issued a "high" severity rating advisory for the WhatsApp users in the country. The advisory is aimed at Android users who use the version of WhatsApp and WhatsApp Business prior to v2.21.4.18, and iOS users who use the version of WhatsApp and WhatsApp Business prior to v2.21.32.

The advisory states that "Multiple vulnerabilities have been reported in WhatsApp applications which could allow a remote attacker to execute arbitrary code or access sensitive information on a targeted system". Further, the advisory explains in detail the vulnerabilities: "exist in WhatsApp applications due to a cache configuration issue and missing bounds check within the audio decoding pipeline".

CERT-In advises WhatsApp users in the country to update their applications to the latest version from the Play Store or Apple App Store so that this vulnerability will not pose a threat to the users.



In another event, the cellphone hacking company Cellebrite developed a method to access the secure mobile messaging app Signal. The Israeli digital forensics firm sells two software packages. The UFED breaks the security levels of iOS and Android phones and collects deleted as well as hidden data. The second one, the Physical Analyzer looks for the presence of digital evidence in the device.

Cellebrite helps private and public investigators in digital investigations. Since Signal is a highly secure mobile IM application and uses the Signal protocol, all conversations through the application are encrypted. After Cellebrite had used their tool to access Signal, the mobile messaging application has then taken adequate measures to avoid any such attempt in the future.

Applications like WhatsApp, Signal, and Telegram offer their users services like end-to-end encryption for improving the app's security. Even though there are security protocols in place to safeguard the privacy and security of the user, it is always better to be vigilant while using mobile chat applications.

While allowing mobile IM applications for business communication between traders and customers, financial firms must always ensure that these conversations are captured and archived. A tool that can capture and record mobile text messages and calls must be used so that no conversation is missed out and regulatory compliance is ensured.

Best Practices to Follow While Using a Mobile Messaging Application

Want more privacy? Use the following recommendations on safe use of messaging apps.

Basic Rules

Lock your phone with a passcode or biometric.

Use messaging apps that encrypt your conversations.

Use messaging apps that verify the ID of contacts.

Refrain from large groups where you're unfamiliar with participants and group admin.

Refrain from using apps where content is available to the service operator.

Did you know?

In Facebook and Telegram you need to start a secret chat to have a fully secure and encrypted conversation.

WhatsApp and Telegram can use metadata to mine and monitor information about groups and interactions you make with others.

In WhatsApp, any group member can download all the contact details of other group members.

Telegram allows you to hide your mobile number from others.

You can automatically blur your face in Signal.

For WeChat, China-registered accounts are under terms of service in the jurisdiction of China and are subject to censorship. Please refrain from getting your contacts into any level of risk.

What's your fear?

If you fear that others will collect information about you or use your information and details, then participate only in groups where you know the group admin and other group members.

If you are concerned about that someone will use the information about who you talk with and the groups you participate, then use less popular chat applications that encrypt the metadata about conversations.

If you fear the content of your conversations getting exposed, then encrypt and lock your mobile phone and your messaging app.

In addition to what has been said above, here is some more information about the most commonly used mobile messaging applications.

As discussed earlier even though Messenger and Telegram offer end-to-end encryption for the conversations, you will have to activate the feature to use it. Despite the fact that WhatsApp and Telegram support encrypted chats, the applications do not encrypt the metadata of the conversations. Hence WhatsApp and Telegram are able to monitor the groups that you participate in, as well as your interactions with other users. Any participant of a group in WhatsApp can download the contact details of all other participants of the same group. Telegram allows you to hide your mobile number from others. Signal offers another unique feature where you can blur the faces on the photos you share. WeChat accounts registered in China fall under the terms of service in China and is subject to censorship. It is therefore not wise to share any inappropriate content using your WeChat account, as it can put you and your contacts at risk.

Additional best practices for keeping your communication private:

Lock your phone – Make sure that your phone is accessible to you and no one else. Use a password or a biometric to lock your phone, so that nobody else can access your phone and tamper with it.

Select the right mobile IM application – A lot of thought must be given while selecting a mobile IM application. And, the factors considered must not be just the easiness of chatting and user experience. Make sure to use a mobile IM application that encrypts your conversations and verifies the ID of contacts.

Stay safe from unknown groups – Since mobile numbers are the basic information to add someone to a group sometimes you may get added to an unknown group or channel. Always stay away from large groups where you don't know the participants or group admin(s). If you are being added to such groups without your consent, then you should leave them as soon as possible.

Avoid apps where service operators have chat access – In some mobile chat applications, the service operators will have access to the chats. This is a hindrance to the user's privacy. Hence, it is wise to avoid the usage of chat applications where the service operator has access to your contacts and chats.

Choose an app having end-to-end chat encryption – End-to-end encryption protects your chats and restricts them from being visible to anyone else, except the intended receiver of the message. Choose a mobile messaging application that encrypts your mobile chats so that more privacy is ensured.

A mobile messaging application that not only encrypts your conversations but also the metadata of your conversations gives you a private and safe chat experience.
While using WhatsApp, WeChat, or any other mobile IM application for enterprise instant messaging, applicable regulations will require you to monitor, record, and archive the conversations through such applications. TeleMessage offers recording and archiving solutions for regulated firms that use popular mobile messaging applications. The adoption of such a solution helps firms maintain regulatory compliance. The tool help firms perform activities like WhatsApp recording, ***WhatsApp archiving***, WeChat recording, and ***WeChat archiving***. TeleMessage will also make available tools capable of ***Signal archiving*** and ***Telegram archiving*** soon so that employees working in regulated firms can have a fully secure mobile messaging experience.

About TeleMessage

TeleMessage captures and retains mobile content, including mobile SMS messages, voice calls, and WeChat and WhatsApp conversations and calls from corporate or BYOD mobile phones to ensure compliance with various data protection regulations. The messages are securely and reliably retained within TeleMessage servers or forwarded to your choice archiving data storage vendor.

Our mobile archiving products securely record content from mobile carriers and mobile devices for various ownership models (BYOD, CYOD, and employer-issued). With our multiple archiving solutions, you can always find the right tools or blend for your requirements:

Network Archiving From Other Carriers

Get text messages from several network carriers into a single archive. TeleMessage is integrated with several leading mobile carrier networks. Get a copy of messages from all these operators into the company enterprise archive.

Android Archiver

Agent for Android that runs in the background and captures all messages and voice calls and uploads them to be archived. Employees can use the native texting app on the phone and get his messages captured and archived.

Enterprise Number Archiver

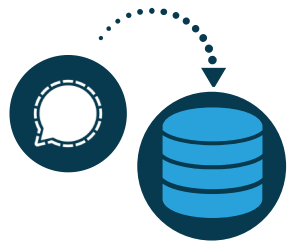
Provides BYOD employees with a business number associated with an App on their Apple or Android smartphones. All business communication done via this 2nd enterprise number is archived.

WhatsApp Archiver

Allow your employees to use the WhatsApp application for iOS and Android while remaining compliant. TeleMessage captures all WhatsApp chats & messages including text, multimedia and other attachments.

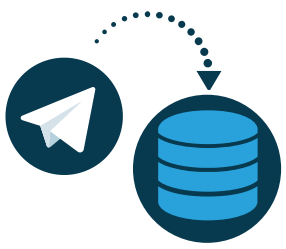
WeChat Archiver

Allow your employees to use the WeChat application for iOS and Android while remaining compliant. TeleMessage captures all WeChat chats & messages including text, multimedia and other attachments.



Signal Archiver

Allow your employees to use the Signal application for iOS and Android while remaining compliant. TeleMessage captures all Signal chats & messages including text, multimedia and other attachments.



Telegram Archiver

Allow your employees to use the Telegram application for iOS and Android while remaining compliant. TeleMessage captures all Telegram chats & messages including text, multimedia and other attachments.

TeleMessage offers cross-carrier and international mobile text & calls archiving for corporate and BYOD phones. Visit our website at **www.telemessage.com** to learn more about our mobile archiving products.

Resources

https://www.calcalist.co.il/internet/articles/0,7340,L-3888113,00.html

https://twitter.com/PrivacyIsrael/status/1348724479321628677/

https://www.kaspersky.co.in/blog/what-is-end-to-end-encryption/21897/

https://www.businesstoday.in/technology/news/indias-cyber-agency-issues-high-severity-security-warning-for-whatsapp-users/story/436889.html

https://gadgets.ndtv.com/apps/news/whatsapp-user-data-breach-leak-security-flaw-vulnerability-cert-in-advisory-2416759