A Comparison of Chat Applications in Terms of Security and Privacy

J. Botha[1], C. Van 't Wout[1], L. Leenen[2]
[1]Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2] University of the Western Cape

[1]jbotha1@csir.co.za
[1] cvtwout@csir.co.za
[2] lleenen@uwc.ac.za

Abstract: Mobile messaging or chat Applications (Apps) have gained increasing popularity over the past decade. Large amounts of data are being transmitted over the internet when people make use of these Apps. Metadata and personal information are being collected and stored every day while consumers are seeking protection against surveillance as well as against attacks from hackers. There are countless Apps available but some are leading the way in popularity, platform availability and features. WhatsApp, one of the leading Apps, revealed in 2016 that it had more than one billion users. In March 2016, WikiLeaks released information that the CIA was able to bypass all security systems of both WhatsApp and Signal, another popular App, to read user messages. WikiLeaks also revealed that the CIA makes use of malware and hacking tools that allow them to remotely hack into smartphones. In 2017, a Guardian report indicated that Facebook, WhatsApp's parent company, could read encrypted messages due to a certain vulnerability found in the App. In terms of security, it is important to distinguish pure secure messaging Apps from the ones who are less secure and trustworthy. This paper compares the best and the supposedly most secure messaging Apps based on the built-in security and privacy features of the Apps, as well as the location and subsequent accessibility of stored data. Recommendations and best practice advisements for users are made on which Apps seem to be the most secure and private.

Keywords: Chat app feature comparison, chat app data storage security, cybersecurity, message encryption, privacy

1. Introduction

Every day millions of people are exchanging messages via messaging or rather chat Applications (Apps). However, users do not know what happens to the messages once they have been sent. Initially, encryption was considered to be used only by paranoid users or people with a heightened need for secrecy. After the revelations of Edward Snowden, consumers have become more aware of online privacy and the dangers of digital scooping of data and identity theft. Surveillance activities are increasing globally and concerns amongst people all over the world has been raised considerably whilst data retention laws are being implemented (Ali, 2017). We live in a digital age where surveillance and data logging occur on almost all our communication. Companies want to collect as much as possible personal information about consumers. Some governments are hacking mobile devices to gain unauthorised access for surveillance and other unknown reasons (Curran, 2018). Recently, the Russian government requested the chat Application Telegram, on several occasions, to give them the encryption keys of citizens registered on the chat Application. Although Telegram did not comply, they are now at risk of being banned in Russia (Caffo, 2018).

Although messaging Apps have been around for a number of years, the development of secure mobile Apps are increasing, focusing on securing the privacy of users and meeting their demands (Corpuz, 2017; Das, 2017). Recent studies show that users are becoming concerned about protecting privacy on their smartphones and opposed apps that collected their contacts (Balebako et al., 2013). One survey of 2, 245 US adults showed that 57% of all smartphone app users have either deleted an app or refused to install an app for security and privacy reasons (Boyles et al. 2012).

This paper covers an overview of the most secure Apps of 2017 and 2018 and also highlight some known security flaws within messaging Apps in Section 2. The main focus is a comparison of these Apps in terms of security and privacy. Section 3 presents a comparison of some of the main security features on a number of the most used messaging Apps. Section 4 provides a comparison of where messaging data and media of Apps are stored and can subsequently be accessed or recovered from. In addition, recommendations are given, in section 5, on the most secure Apps to use as well as best practices for back-ups. The paper concludes in section 7.

2. An Overview of the Best and Most Secure Messaging Apps

This section gives an overview of the Apps that are regarded to be the best and the most secure; Facebook, WhatsApp, Telegram, Signal, WeChat, Line, Skype and Viber (Caffo, 2018). Two of the main reasons why chat Applications have become so popular at a rapid pace, are firstly, the rapid growth in access to cell-phones and to the Internet. Secondly the death of SMS messages because chat Applications allow for "richer" methods of remote communication.

Facebook's chat Application is called Messenger. This App is used by over two billion users registered on Facebook. The App can be accessed via Facebook and allows for normal chat messages, voice and video calls. End-to-end encryption is not enabled by default and has to be enabled with each and every chat by selecting the Secret Conversation option when messaging a contact. WhatsApp (WhatsApp, 2019) has a simple installation and setup by synchronising contacts on your phone automatically. It allows for text and multimedia messages with end-to-end encryption by default. It also periodically asks for a password to access the App. WhatsApp is owned by Facebook and there are rumours that Facebook intends to populate members' Facebook profiles with their WhatsApp data. This idea has been blocked by the European Union, but it seems it is only a matter of time before this feature might be built in, posing more security and privacy risks to users (Caffo, 2018). WhatsApp is the most popular messaging App (Sutikno et al., 2016).

Telegram (Telegram, 2019) was launched after the Snowden revelations for user that are aware of the need for secure digital communication. It offers a client-server encryption for chat messages and secret chats where privacy cannot be violated. These chats self-destruct after a certain time on the devices at both ends (for both individual or group chats) as well as on the server.

Signal is developed by a company called Open Whisper Systems. Edward Snowden stated that this company can be trusted*: "Use anything by Open Whisper Systems"*. The App uses military-level end-to-end encryption. Signal is strengthened by an open-source platform, which is closely monitored and reviewed to improve security. It is the preferred App for hacktivists and leading security experts (Signal, 2019).

WeChat has more than 700 million users and dominates the Chinese web. The App offers text messages, voice and video calls, group chats and a rich multimedia experience. It also offers features such as "Friend Radar", "People Nearby" and "Shake" to find new people online. It was one of the first Apps that was available on Android Wear and Apple Watch. It does not offer end-to-end encryption, but it does provide client-to-server and server-to-client protection. The App has an accreditation from the Privacy company TRUSTe, who provides solutions to manage privacy compliance for the General Data Protection Regulation (GDPR) and other global privacy regulations (TRUSTe, 2019). WeChat also complies with **ISO 270001-2013**, a very strict international standard, therefore it would be very difficult for hackers to breach the Application (Caffo, 2018).

Line is a Japanese App with more than 600 million users globally. Line offers additional features such as group chats and calls of up to 200 participants and allows calling of mobile and landline numbers via purchased credits. It also follows certain channels, news feeds and events. Skype was recently revamped in an attempt to make it more attractive to users. It is still known for its great audio and video capabilities and is used more by corporate users. Digital communication is secured by Transport Layer Security (TLS) and Advanced Encryption Standard (AES) encryption; however, there is no encryption when calling landline or mobile numbers (Websecurity.symantic.com, 2019). Viber has similar features to WhatsApp by using a mobile number to login and syncing contacts on the phone book of the device (Caffo, 2018; Viber, 2019).

Table 1 provides a summarised comparison of these Apps in terms of security and privacy features. According to the Amnesty International report of 2016, Snapchat ranked among the least secure Apps because it fails with respect to privacy by not implementing end-to-end encryption (Williams, 2016). In 2019, Snapchat announced that end-to-end encryption has been added to protect user's messages (Titcomb, 2019).

3. Comparing Security and Privacy Features

Since consumers demand better security and privacy in messaging Apps, software development companies have been attempting to address these issues. One of the features was to launch end-to end-encryption (see Figure 1). End-to-end encryption refers to when messages are encrypted during transmission and no copy is stored unencrypted on the servers of the service providers. Nobody apart from the people communicating can view these messages party; no third party, not even the government or the developers of these Apps. Communication is transmitted using a secret code rather than plain text (Rijnetu, 2018).

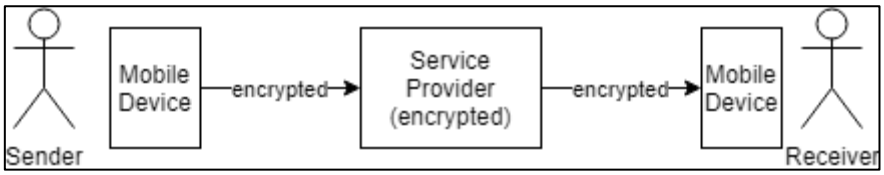

Figure 1. End-to-end Encryption

Another type of encryption that is used is encryption in transit (see Figure 2). This means the message is encrypted between the user and the service provider, but stored as clear text on the server. This poses a risk as stored messages can be read by the service provider or other third parties that gain access to the server.

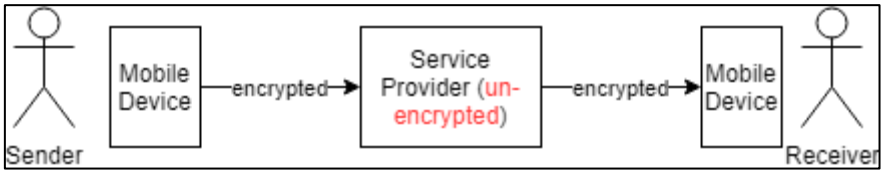

Figure 2. Encryption in Transit

Table 1 presents a comparison on messaging Apps with regards to security and privacy features.

Table 1. Security and Privacy Features of Messaging Apps

Messaging App	End-to-end encryption	Encryption in Transit	Private key not accessible by provider	Deleted from Server	Self-Destruct Messages	Open-Source	Password lock	Verification SMS/Email	Screenshot detection	Two-step Verification	Remote logout	Remotely Wipe Messages	Account self-destruct	Free
Confide	✓							✓						
CoverMe	✓				✓							✓		
Dust	✓			✓	✓				✓					✓
Hangouts		✓												✓
iMessage	✓		✓	✓	✓									✓
Line	✓							✓						✓
Messenger	✓(optional)	✓			✓									✓
Signal	✓				✓	✓	✓							✓
Skype	✓(optional)	✓												✓
Slack		✓												✓
Snapchat	✓													✓
Telegram	✓(optional)	✓	✓		✓	✓	✓			✓	✓		✓	✓
Threema	✓													
Viber	✓		✓	✓	✓		✓							✓
WeChat														✓
WhatsApp	✓		✓				✓	✓				✓		✓
Wickr Me	✓								✓					

Apps are sorted alphabetically

One can argue that an adequate level of **end-to-end encryption** should be the golden standard and default security feature to be included in messaging Apps. Most Applications listed in Table 1 provide end-to-end encryption. Signal, WhatsApp and Facebook Messenger make use of the Signal end-to-end encryption protocol. Although Telegram, Skype and Messenger offers end-to-end encryption, it is not enabled by default. Telegram offers this feature as a "secret chat" option. If this is not enabled, encryption in transit is used. Skype recently added end-to-end encryption, but it is not on by default. One has to start a "private conversation" to enable end-to-end encryption (Deahl, 2018). Secret conversations on Messenger are currently only available in the Mobile App; it will thus not Appear on Facebook chat or messenger.com and is furthermore only visible on the device where you create the conversation and the device the recipient uses to open the conversation (Woollaston, 2016). Therefore, Messenger, Skype and Telegram has checks for both end-to-end and in-transit encryption as seen in Table 1. (End-to-end encryption by default encrypts in transit as well).

Hangouts and Slack does not provide end-to-end encryption, but instead make use of **encryption in transit.** This immediately makes them less secure and trustworthy. According to (Corrigan, 2018), Google Hangouts is an App that

should be avoided. The App allegedly has numerous security and privacy concerns. It uses encryption in transit, messages are stored on the server in clear text. Google can access anyone's private messages at any time and relay the information to government agencies and other third parties (Corrigan, 2018). According to the 2016/17 Amnesty International Report (Amnesty.org, 2017, Griggs, 2018), WeChat has major privacy issues. They ranked last with a score of zero out of 100 when it comes to privacy. Facebook Messenger and WhatsApp scored 73 and Apple's iMessage 67 out of 100 (Griggs, 2018). WeChat provides no end-to-end encryption and did not publish transparency reports on China's government request for information. Based on this, WeChat was subjected to both censorship and surveillance. Due the lack of privacy and security in WeChat, it is safer to delete the App from your device.

Since most of the Apps make use of end-to-end encryption, the next concern that arises is to know if the **private key is accessible by the service provider**. Apple, Telegram and WhatsApp claim that they cannot obtain the private key. No information was found on the remaining Apps in Table 1. Although Apple claims they cannot access the private key and are unable to read the user's messages, a study done by Hackers indicated otherwise. They proved that technically Apple can read your iMessage messages whenever they want to (Blue, 2018). One concern is that Confide does not notify users if the primary when a new key is generated, whereas Apps does as iMessage and WhatsApp do alert users on this (TechCrunch, 2017).

iMessage, Viber and Dust are the only chat Apps that claim they **delete your messages from the server.** iMessage delete messages automatically after seven days from the server (Corrigan, 2018). Dust has a feature of never permanently storing your message on the server (Rijnetu, 2018). The message is stored in the random-access memory (RAM) of the server. Once the receiver has received the message, the message gets removed from the RAM. Dust also allows to erase messages from the receiver's device sent by the particular sender. Telegram, iMessage, Viber, Messenger, CoverMe, Dust and Signal have a feature that allows for the messages to **self-destruct or disappear** after a certain amount of time for both the sender and recipients' devices (Corrigan, 2018). Facebook is rolling out a self-destruct timer for messages that allows users to set a timer that will have messages disappear automatically (Woollaston, 2016).

Both Signal and Telegram have an **open-source** policy. Anyone can check the source code, protocol and API (Corrigan, 2018). With Threema, only the encryption part of the source is open, the rest is not open source (Decentralize.today, 2016). Signal, Telegram, Viber and WhatsApp has a **pass-code lock** on the chat App that one needs to enter before the App can be used (Corrigan, 2018). On registration of a new user, both WhatsApp and Line send a **verification code via SMS** that is required before the installation can be completed (Corrigan, 2018). Dust and Wickr Me introduced a new feature, **screenshot detection,** that notifies the user when a screenshot has been made of a chat sent by that particular user (Corrigan, 2018). Telegram offers a **two-step verification** feature where the App requires to use both a SMS code and password to log into the App. The App also allows for setting up a recovery email address for in case a user forgets the password (Corrigan, 2018). **Remote logout** is a feature offered by Telegram only. Most Apps allow to be logged into the App from multiple devices. With this feature one can logout from all devices from the current device in use (Corrigan, 2018). Another feature is the account **self-destruct**. Only Telegram offers this functionality. If the account has been inactive for a certain period, where six months is the default, the account will automatically self-destruct and all messages and media linked to the account will be erased (Corrigan, 2018).

Most of the Apps compared in Table 1 are free of charge. Apps such as Slack and Threema may be more suitable for private business chats, whereas the other Apps are aimed at personal use. It seems as if a new market has opened for the development of more secure Apps and to charge users for the secure chatting service. Such Apps, which are not free of charge are Threema, Wickr Me, CoverMe and Confide. Wickr Me has a free version with limited functionality but the professional version is not free of charge. CoverMe has additional features to the ones compared to in Table 1, such as a private vault to lock your messages, passwords, documents and multimedia; it allows users to obtain a second private number to hide the callers personal number; military-graded encrypted phone calls, password protected call pickups; and it allows to disguise and hide the App with a news reader App for example (CoverMe, 2019).

The results in this section indicate that Signal, Telegram, WhatsApp and Viber are the most secure free Apps. All the paid for Apps in Table 1 include all of the basic security and privacy features as well as additional features, indicating that they might be more secure than the secure free Apps. CoverMe has taken the security and privacy to the next level with a number of additional features to hide and disguise the user's information. The least secure Apps are WeChat, Google Hangouts and Slack primarily due to not using end-to-end encryption. The next section compares the Apps in terms of accessibility of stored data.

4. Comparing Accessibility of Stored Data

The next question in the comparison of messaging Apps in terms of security and privacy is where the data is stored and how easily it can be recovered – this would include chat history, messages, photos and videos sent via these Apps. This section compares messaging Apps based on this factor. The Apps (free versions) that were found to be the most secure from section 3, Table 1, are being compared in Table 2. LINE and WeChat were also added to this comparison, due to their popularity in the east.

Table 2. Location of Stored Chat App Data

Apps	Device Back-up: Chat History	Device Back-up: Images & Videos	Cloud Back-up	Back-up to PC	Transfer Chat history between mobile devices	Copies sent to email
LINE	✓	✓	✓(optional)	✓(optional)	✓	✓
Signal	✓	✓			✓	✓
Telegram	✓	✓	✓(optional)	✓(optional)	✓	✓
Viber	✓	✓	✓(optional)	✓(optional)	✓	✓
WeChat	✓	✓	✓(optional)	✓(optional, default on web-version)	✓	✓
WhatsApp	✓	✓	✓(optional)	✓(optional, default on web-version)	✓	✓

Apps are sorted alphabetically

LINE allows users to choose to back-up the chat history in various places: LINE Keep or Memo (on device), share to email, Google Drive, OneDrive and to PC (Bruce, 2017). The app has optional features to back up on the cloud and on a PC. **Signal** only stores the metadata on the device that is required for the App to work. Signal does allow for a backup on the device as optional, but no PC, server or cloud backup is provided (Support.signal.org, 2019). **Telegram** stores all images on the image folder on the device internal storage or SD card. Deleted chats, images and videos are also stored in the cache folder of the SD card (Coline, 2016). Telegram stores all chats and media on their cloud service. Secret chats are not stored on the server, but secret media do get stored (encrypted).

Viber allows users to save a copy of their chats by sending it to their email via the user settings. Chats will be put into an archived .zip folder as .csv files with the names of contacts that you chatted to. A chat backup copy can be created and read as text, but it cannot be restored in the Application itself; copies of sent files (photos, videos etc) are not saved to such text files. Viber also keeps data in a separate folder located in the internal system memory of the user's device. Such backup data can be accessed only with Root rights or by using a kind of Root explorer software (Cherniga, 2017).

WeChat data can be backed up on a personal computer (PC) using WeChat Client software downloaded from the internet. WeChat, as well as other Apps (e.g. WhatsApp, Line, Kik, Viber, etc), data can also be backed-up to PC using USB connection and dr.phone software without internet connection. A back-up may also be made by data transfer to another smartphone (Dr.phone, 2019). The Cloud backup feature is no longer available from WeChat 6.2.5. Chat history is kept permanently within the App on the device for as long as the App is not removed, and the phone has sufficient storage space. In the interest of privacy, WeChat does not store the chat history on its server unless a user explicitly chooses the backup feature. Chat history cannot be recovered once deleted (WeChat Help Center, 2019).

WhatsApp data is stored on the device of the sender and receiver. Backups are made on the user's device by default on a daily basis within the internal storage and backups may also be stored on the user's Google Drive. Back-up media and messages are not protected by WhatsApp end-to-end encryption while in Google Drive (WhatsApp FAQ, 2019). Messenger data is stored in the user's Facebook account. Message history of all messages created, whether on the Facebook website, Messenger for PC or for Android, is always transferred through the Facebook account and saved there. Facebook provides users with the opportunity to save a copy of all user information, including uploaded images and videos, contact information, friends and most importantly, the complete message history (Hetman Software, 2019).

Messenger data is also stored to Android devices in the same manner as similar Apps (e.g. Whatsapp) in the internal storage or SD card Android's data folder (Anydata Recovery, 2019).

All Apps in Table 2 backs up the data on the device. Signal is the only App that does not allow backup to a PC or Cloud, all other Apps has this as an optional feature. All Apps allow to transfer messages from one mobile device to another. All of the Apps allow to send chats to email, unencrypted. This poses a risk for if a user's email gets compromised, all of the chat backups will be available to the attacker. Based on the finding in this section, Signal would be the most secure option due to the App not allowing backups on the cloud or on a PC. All the Apps allow this feature as optional, therefore, if this feature is not used, they would be on par with Signal in this comparison.

5. Recommendations

The data generated on and transmitted via messaging Apps may be vulnerable in terms of privacy and confidentiality. This paper compared messaging Apps based on the built-in security features of the Apps, as well as the location and subsequent accessibility of stored data. Recommendations are made for users to maintain privacy and confidentiality based on these two aspects.

Based on the findings in sections 3 and 4, the best and most secure free chat Apps are Signal, Telegram, WhatsApp, Viber and Line. WeChat is ruled out due to privacy concerns highlighted in section 3.

Users often have a need to recover their chat history or data and can hence make use of the back-up functions of the various Apps to enable later restoring or recovery of data. Such back-ups are usually stored on the device itself and/or somewhere in the cloud. Users have further options on the different Apps to make back-ups to email or on their PC. If devices contain classified information (personal or otherwise) the required security controls should be applied to ensure that the data is "safe" in case the device or PC gets compromised.

The choice of which messaging App is best depends on criteria that have varying importance to different users and also influences the required level of security. Such criteria include:

- Being able to connect with relevant others.
- Various countries use different Apps.
- Availability (if there is internet, there is messaging App). No available cellular phone minutes and exorbitant fees can also be relevant factors.
- Cellular phone service provider does not own messaging App data – therefore messaging App data is already more secure than SMSs.
- It would not make sense to the average person to switch to some very secure paid App if the people they need to engage with are not using the same App. It may be relevant for a business organisation to use such an App for communication between colleagues in order to protect information assets.

Users are therefore recommended to apply the correct settings in the use of their preferred messaging App, depending on whether they have a need to recover chat history and other media generated on these Apps. The safest option is not to backup chats and media to a PC or cloud service. If a device containing backups is lost, all backups are lost with it.

The forensic community uses tools enabled to access well-known Session Initiation Protocol (SIP) and Voice over Internet Protocol (VoIP) which Applies to messaging Apps. Forensic recovery of important data is thus possible for some messaging Apps. This also implies that if users need to be more secure, they should make use of a less common App. This has its own challenges on the other hand, because it is not exactly clear where the servers are that store the data from these less known Apps.

6. Conclusion

People choose messaging Apps based on different criteria and would hence have different requirements in terms of levels of security (confidentiality and privacy of their chat data). Users are recommended to apply the correct settings in the use of their preferred messaging App, depending on whether they have a need to recover chat history and other media generated on these Apps.

A comparison of the security features of various Apps suggests that Signal, Telegram, WhatsApp and Viber are the most secure free Apps. All of the paid for Apps in Table 1 seem to be equally as secure or even more secure than the most secure free Apps. CoverMe has taken security and privacy to the next level with a number of additional features to hide and disguise the user's information. The least secure Apps are WeChat, Google Hangouts and Slack, primarily due to not using end-to-end encryption. It has been highlighted that WeChat has major privacy issues and the safest option is to remove the App from your phone. Google Hangouts was also flagged for numerous security and privacy concerns.

A comparison in terms of the accessibility to stored App data suggest that Signal is the most secure. On the remainder of the Apps in Table 2, if the correct user settings are applied for back-up of data, they would be on par with Signal with regards to the storage and backup of data. The least secure Apps in Table 2 are WhatsApp and WeChat, primarily due to the fact that if the web-version is used, chats and media gets backed up on the PC by default.

References

Ali, Z. (2017). Best Secure Messaging Apps for Android and iOS - PrivacyEnd. Available at: https://www.privacyend.com/best-encrypted-messaging-Apps./ [Accessed 15 Jan. 2018].9

Amnesty.org. (2017). Amnesty Internation Report 2016/17. Available at: https://www.amnesty.org/download/Documents/POL1048002017ENGLISH.PDF [Accessed 10 Apr. 2019].

Anydata Recovery (2019). How to Recover Deleted Facebook Messenger Messages on Android Device. Available at https://www.any-data-recovery.com/android-data/recover-deleted-facebook-messenger-message-from-android-devices.html [Accessed 11 Apr 2019].

Balebako, R., Jun, J., Lu, W., Cranor, L.F., and Nguyen, C. (2013). "Little Brothers Watching you": Raising Awareness of Data Leaks on Smartphones. Proceedings of the Ninth Symposium on Usable Privacy and Security.

Blue, V. (2018). Hackers: Here's how Apple's iMessage surveillance flaw works (video). Available at: https://www.zdnet.com/article/hackers-heres-how-Apples-imessage-surveillance-flaw-works-video/ [Accessed 15 Mar 2019].

Boyles, J.L., Smith, A., and Madden, M. (2012). Privacy and Data Management on Mobile Devices. Pew Internet and American Life Projects.

Bruce, I. (2017). Ways to Back Up and Restore LINE Chat on Android. Available at: https://www.recovery-android.com/backup-restore-line-android.html [Accessed 15 Mar 2019].

Caffo, A. (2018). The best (and most secure) chat Apps. Available at https://blog.avira.com/best-chat-Apps-smartphone [Accessed 7 Mar 2019].

Cherniga, M. (2017). How to Recover Message History, Contacts and Viber Files on Android or Windows. Available at: https://hetmanrecovery-com.cdn.ampproject.org [Accessed 15 Mar 2019].

Coline, N. (2016). How Can I Recover Deleted Telegram Chats? Available at: https://www.quora.com/How-can-I-recover-deleted-Telegram-chats. [Accessed 15 Mar 2019].

Corrigan, C. (2018). The very best private messaging Apps. Available at https://www.avg.com/en/signal/secure-message-Apps. [Accessed 9 April 2019].

Corpuz, J. (2017). Best Encrypted Messaging Apps. Available at: https://www.tomsguide.com/us/pictures-story/761-best-encrypted-messaging-Apps.html. [Accessed 15 Jan. 2019].

CoverMe (2019). Corporate Websites. Available at: http://www.coverme.ws/en/index.html. [Accessed 10 Apr. 2019].

Curran, D. (2018). Are your phone camera and microphone spying on you? The Guardian. Available at: https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying [Accessed 14 Apr 2019].

Das, A. (2017). 8 Best Secure and Encrypted Messaging Apps for Android & iOS. Fossbytes. Available at: https://fossbytes.com/best-secure-encrypted-messaging-Apps. [Accessed 15 Jan 2019].

Deahl, D. (2018). Skype now offers end-to-end encryption conversations. Available at: https://www.theverge.com/2018/8/20/17725226/skype-private-conversation-end-to-end-encrypted-opt-in. [Accessed 10 Apr. 2019].

Decentralize.today (2016). Threema – Secure Messengers..or not so secure? Part 3 Available at: https://decentralize.today/threema-secure-messengers-or-not-so-secure-part-3-6df427896caa. [Accessed 10 Apr. 2019].

Dr.fone (2019). How to Backup WeChat: 5 Ways You May Not Know. Available at: https://drfone.wondershare.com/wechat/wechat-backup.html. [Accessed 15 Mar 2019].

Grigg, A (2018). WeChat's privacy issues mean you should delete China's No. 1 messaging App. Available at: https://www.afr.com/news/world/asia/wechats-privacy-issues-mean-you-should-delete-chinas-no1-messaging-App-20180221-h0wgct. [Accessed 20 Mar 2019].

Hetman Software. (2019). How to Save or Restore Facebook Messenger Access and Data on Android or PC. Available at: https://hetmanrecovery.com/recovery_news/how-to-save-or-restore-facebook-messenger-access-and-data-on-android-or-pc.htm [Accessed 10 Apr 2019]

Kim, L. (2018). The Top 7 Messenger Apps in the World. Available at: https://www.inc.com/larry-kim/the-top-7-messenger-Apps-in-world.html. [Accessed 15 Mar 2019].

Messenger (2019). Corporate Website. Available at: https://www.messenger.com. [Accessed 7 Mar 2019].

Pryvate (2019). Corporate Website. Available at: https://www.pryvatenow.com. [Accessed 7 Mar 2019].

Rijnetu, I. (2018). The Best Encrypted Messaging Apps You Should Use Today. https://heimdalsecurity.com/blog/the-best-encrypted-messaging-Apps. [Accessed 25 Mar 2019].

Signal (2019). Corporate Website. Available at: https://signal.org. [Accessed 7 Mar 2019].

Support.signal.org (2019). Signal Support Website. Backup and Restore Messages. Available at: https://support.signal.org/hc/en-us/articles/360007059752-Backup-and-Restore-Messages. [Accessed 12 Apr 2019].

Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M.A. and Subroto, I.M.I., 2016. WhatsApp, viber and telegram: Which is the best for instant messaging? International Journal of Electrical & Computer Engineering (2088-8708), 6(3).

TechCrunch.com (2017). Researchers critique security in messaging App Confide. Available at: https://techcrunch.com/2017/03/08/researchers-critique-security-in-messaging-app-confide/ [Accessed 12 Apr 2019].

Telegram (2019). Corporate Website. Available at: https://telegram.org [Accessed 7 Mar 2019].

Telegram.org/privacy (2019). Telegram Privacy Policy. Available at: https://telegram.org/privacy [Accessed 12 Apr 2019].

Titcomb, J (2019). Snapchat adds end-to-end encryption to protect users' messages Available at: https://www.telegraph.co.uk/technology/2019/01/09/snapchat-adds-end-to-end-encryption-protect-users-messages [Accessed 9 April 2019].

TRUSTe (2019). Corporate Website. Available at https://www.trustarc.com/ [Accessed 7 Mar 2019].

Viber (2019). Corporate Website. Available at: https://support.viber.com. [Accessed 7 Mar 2019].

WhatsApp (2018). WhatsApp Encryption Overview – Technical White paper. Available at: https://www.whatsApp.com/security/WhatsApp-Security-Whitepaper.pdf. [Accessed 15 Jan 2019].

WhatsApp (2019). Corporate Website. Available at: https://www.whatsApp.com. [Accessed 7 Mar 2019].

WhatsApp FAQ (2019). Restoring Your Chat History. Available at: https://faq.whatsApp.com/en/android/20887921 [Accessed 15 Mar 2019].

Websecurity.symantic.com (2019). The Ultimate Guid: What is SSL, TLS and HTTPS. Available at: https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https. [Accessed 7 Mar 2019].

WeChat (2019). Corporate Website. Available at: https://www.wechat.com. [Accessed 7 Mar 2019].

WeChat Help Center (2019). Chat History. Available at: https://help.wechat.com/cgi-bin/newreadtemplate?t=help_center/topic_list&plat=2&lang=en&Channel=helpcenter&detail=1001146. [Accessed 15 Mar 2019].

Williams, R. (2016). Snapchat among least secure Apps for data protection, report finds. Available at: https://inews.co.uk/news/technology/snapchat-among-least-secure-Apps-data-protection-report-finds. [Accessed 7 Mar 2019].

Woollaston, V. (2016). How to find and use Facebook's Secret messages. Available at: https://www.wired.co.uk/article/messenger-secret-messages-end-to-end-encryption [Accessed 15 Mar 2019].