TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Erik-Filipp Oleinikov 179920IVSB

Comparison of Security and Confidentiality Aspects in Modern Messenger Applications

Bachelor's thesis

Supervisor: Mohammad Tariq
Meeran
PhD

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Erik-Filipp Oleinikov 179920IVSB

Kaasaegsete messenger-rakenduste turvalisuse ja konfidentsiaalsuse aspektide võrdlus

Bakalaureusetöö

Juhendaja: Mohammad Tariq
Meeran
PhD

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Erik-Filipp Oleinikov

10.05.2021

Abstract

This work was written in order to help non-IT users understand the basic principles of messengers, their differences and similarities in security and privacy aspects, and also, help to choose the best messenger that can provide convenience, as well as a good level of security and privacy.

In the course of this work, the most popular messengers are described and explored, as well as all materials related to their privacy, security, known vulnerabilities and data leaks, are collected in order to compile a detailed comparison table of all messengers to determine the most secure and private of them. After that, a survey is conducted among a group of people who use instant messengers in order to determine which aspects are most important to them and what is their attitude towards privacy and security in general. Based on the responses of the focus group, the most optimal messenger is selected, which will suit the respondents but will also be safe and private. Thus, considering the technical characteristics of messengers and their functionality, as well as the desires of the respondents, the author proposes the most suitable option.

This thesis is written in English and is 59 pages long, including 5 chapters, 32 figures and 1 table.

List of abbreviations and terms

GPS	Global Positioning System
IM	Instant messaging
SMS	Short message service
VoIP	Voice over Internet Protocol
XMPP	Extensible Messaging and Presence Protocol

Table of contents

List of figures

1 Introduction

In the modern world, instant messengers are becoming more and more popular. Security and privacy play an important role when choosing an application in which to discuss sensitive topics. Having a reliable and secure messaging application can ensure confidentiality of data.

The goal of this thesis is to determine the best options when choosing a messenger in terms of security and privacy, while considering the demands and preferences of the focus group.

Nowadays, not all messengers are safe to use or transfer confidential data. Also, many messengers intentionally collect data and have their own privacy policy, with which the user must agree to use the messenger. This work will consider the most popular messengers and will analyze their privacy and security functions, as well as consider all the privacy policies, vulnerabilities, and data leaks that each messenger recently had.

In the course of the study, users of messengers will also be interviewed in order to find out their attitude to privacy and security, as well as the functions that they consider the most important. Based on the opinion of the respondents and the studied information about each messenger, the most suitable options for private and secure communication will be selected for a focus group.

The main questions of the author are:

- What are the differences between popular instant messengers?
- Which messengers are the most private and secure?

The author will try to find answers to all these questions and reveal the topic in order to determine the best option for reliable communication and data transfer.

2 Methodology

The research methodology will be divided into two parts. Firstly, the author will describe all selected messengers in terms of security and privacy. All messengers are selected by the worldwide popularity. The second part is a comparative study and will consist of creating a table to compare privacy and security of chosen messenger applications, as well as analyzing the survey to determine which preferences people have.

2.1 Comparative Study

The comparative study was chosen in order to understand and see the difference between modern instant messengers. IM applications are very different and have their own set of features and disadvantages. Drawing up a table and conducting a comparative analysis in this case will help to clearly demonstrate the basic differences between messengers in terms of their common or unique features. [1].

2.2 Questionnaire

The compilation of the questionnaire and the conduction of the survey were chosen in order to find out the opinion of users and their attitude towards various messengers, as well as their opinion on security and privacy. Also, to find out their preferences in the functions and capabilities of the application itself. It is the questionnaire that is the ideal method, since it allows to quickly and effectively collect the opinion of respondents and compare it with the existing facts [2]. Since the purpose of the work is to help in choosing the best option to ensure privacy and security, it is needed to consider not only the functions themselves, but also the wishes and opinion of people who use messenger applications. If the messenger is very secure but not usable and convenient for people, there would be no meaning in advising such messenger.

To efficiently analyze the data, respondents were questioned on the topic of the most needed security and privacy aspects, as well as their attitude towards confidentiality of data. Then, having the comparative table and including all the data gathered from description of the most popular messengers and the demands of people, it is possible to visually demonstrate which messenger would be the most fitting for the focus group in terms of security and privacy.

3 Most Popular Messenger Apps

3.1 Messenger Application

Messenger apps are based on fast messaging and uninterrupted contact with each other. When sending messages, each messenger is guided by its own set of security and cryptography rules, as well as a confidentiality agreement. Nowadays, there are many instant messengers such as Telegram, WhatsApp, Facebook Messenger, Viber, WeChat, Signal and many more, but not all of them are safe for transferring personal data and conducting private conversations. [3]

3.1.1 The Basic Principle of Operation of Messaging Applications

Throughout the years, messenger applications have evolved into a multifunctional platform and now they perform not only the basic function of sending messages, but also allow clients to make voice and video calls, transfer files, record audio or video messages, make monetary transactions or even host a huge media channels for a huge auditory.

Messaging applications use IM techonology that allow clients to have real-time conversations over the Internet and for the proper work of IM application, a persistent Internet connection is necessary. IM uses different protocols that can ralay on a client-server or peer-to-peer architecture, depending on the needs of messaging application. Most of the popular messengers use client-server architecture to allow the possibility to connect people over great distances or have all their conversations stored and make them easy accessible from a wide range of devices [4][5]. Client-server architecture helps to divide tasks between servers and clients, allowing servers to handle the user request through a client application on a device.

The division for server and client goes as follows: User needs to download a particular application and register an account. Basically, a phone number, username or email is used for this process. A server works as a relay between such clients and allows them to exchange messages. It is for a particular company to decide, whether they store all the chats on the server itself and then synchronize it with each client or to have all chats stored on each client device and use the server especially for the authentication and relay functions. For the security reasons, some applications use end-to-end encryption and store the encryption keys on each client device, while the server receives and sends each encrypted message to a corresponding contact. [5][6] The client-server architecture is illustrated on the Figure 1

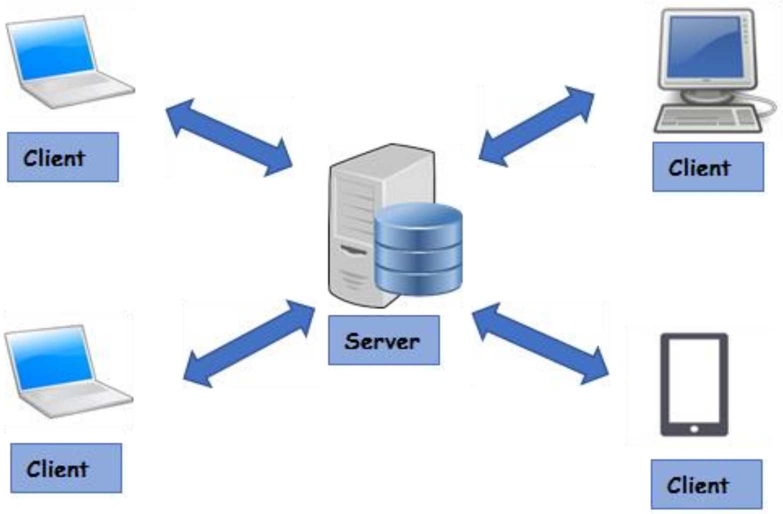


Figure 1 The Client-Server Architecture (Source: https://www.omnisci.com/technical-glossary/client-server)

On the other hand, some applications use peer-to-peer architecture and instead of using a centralized server, the clients can exchange messages directly and perform server and client functions simultaneously. [5][7] The peer-to-peer topology can be seen in Figure 2.

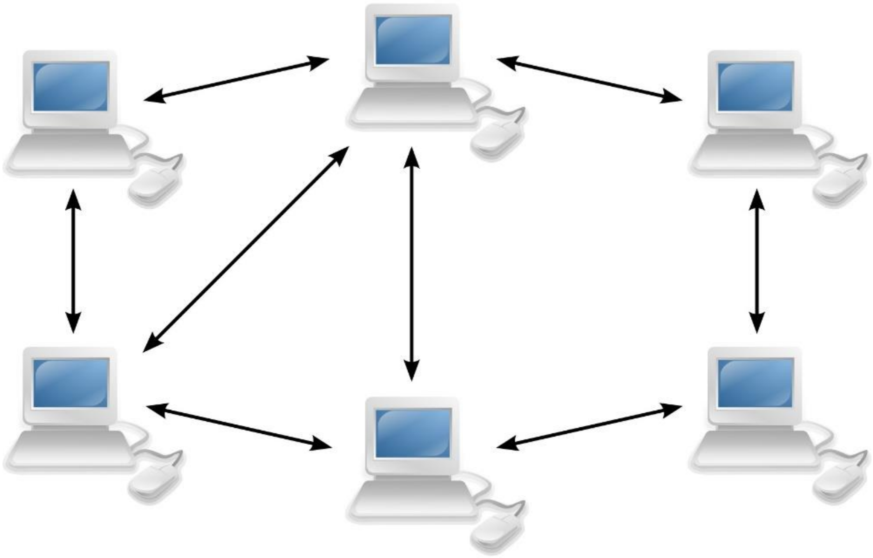


Figure 2 Peer-to-Peer architecture (Source:https://www.cyberagentsinc.com/2018/09/14/peer-to-peer-networks/)

3.1.2 Most Popular Representatives

With the development of IM applications, the variety of apps increased and today there are many clients that are popular and widely used across the globe. Some of these client apps are Facebook Messenger, WhatsApp, WeChat, Telegram and many more. According to the statistics, in 2021 the most popular messaging app is WhatsApp client with 2 billion monthly active users, and that is only one messenger. [8] Figure 3 shows the full statistics of the most popular messengers.

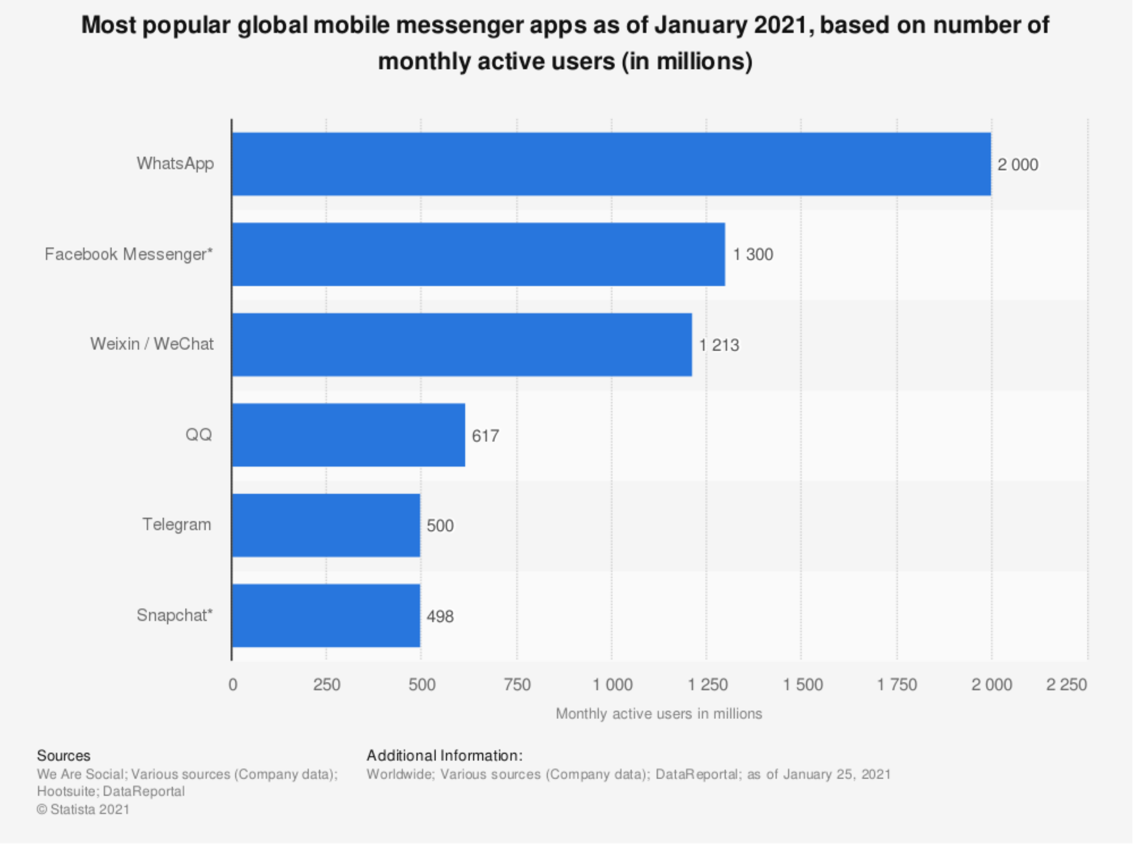


Figure 3 Most popular global mobile messenger apps as of January 2021 (Source: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/)

3.2 WhatsApp

3.2.1 Description of WhatsApp

WhatsApp is by far the most popular multifunctional messenger application that was founded and released by Jan Koum and Brian Acton in year 2009 [9]. In year 2014 WhatsApp was sold to Facebook Inc. for $19 billion dollars, but still continues to function independently from Facebook Messenger as a second IM project [9][10]. WhatsApp application offers a wide range of function such as: messaging, calling, sharing photos, videos, documents and location, making monetary transactions etc. [9]

3.2.2 Security Settings and Options

WhatsApp has at its disposal a number of basic functions inherent in most instant messengers:

- Two-step verification is an optional feature that was introduced in year 2017 and plays an important role in accessing or restoring your account. This feature can be enabled through messenger options menu and will ask a user to provide his e-mail address and set up a PIN code. If user forgets his PIN code it is possible to restore access through an e-mail and set up a new PIN. Without having access to registered e-mail, it is not possible for a third person to access user's account. If the user himself loses an access to his e-mail, then it is needed to recover an account using WhatsApp support page and wait 7 days. [11][12][13]

- Disappearing Messages is one of the recent features that was introduced in 2020. It allows users to have more control over their chats and its history. While enabling Disappearing Messages function, all chats that are stored on each device will be deleted after 7 days. This feature works in group chats as well, but only the admin has the full control and can enable this function for the whole chat. WhatsApp media like photos or videos are automatically deleted as well. [14][15]
- Fingerprint Lock feature allows WhatsApp application to additionally ask for a fingerprint, Touch ID, or Face ID verification before accessing your chats. [16][17]
- Security Code Change Notification feature allows WhatsApp users to verify that their chats are encrypted and secured. Each chat has its own unique code that can be seen on both sides of the conversation. If the codes are identical – chats are secured, and encryption is working properly. In the cases when a device has been changed or account has been restored, a corresponding notification will be seen on both sides of the chat. [18]
- Suspicious Links feature allows to check if the link is malicious or not. Unusual combinations of character in links will be considered suspicious and an alert message will be displayed to notify the user. [19]

3.2.3 Encryption of WhatsApp

WhatsApp uses end-to-end encryption by default on all its media including messages, photos, videos, documents, voice messages and even calls. For the encryption WhatsApp application uses Signal encryption protocol. End-to-end encryption ensures that only the users of the same chat conversation can decrypt and read the messages. Both private and public keys for encryption and decryption are stored on each separate device and not on the servers. This method ensures that even if the data will be intercepted, it is not possible for a third-party to decrypt the messages and read them. Keys for end-to-end encryption are unique and can be used only for a one specific chat. To ensure that messages are encoded, and end-to-end encryption is activated both ways, unique security codes are used. If the security codes on both sides of the chat are identical, then end-to-end encryption works properly. [20][21]

3.2.4 Issues of Security Features

Just like every application, WhatsApp has its weak sides in terms of security. Despite having strong end-to-end encryption, it cannot provide ideal security in every aspect. Even when the server itself cannot decrypt or read chat messages, it still receives and stores the data about the time, date and the contact of each message that went through. Also, storing all the data, chats and encryption keys on a single device can be dangerous. If someone could get full access to a particular device without two-step verification, then it is possible to read all the messages or steal the data. [22]

Additional security with fingerprint lock can be useful but still violated using data breaches, inaccuracies or even use of force. [23]

WhatsApp Payments feature enables the user to transfer money between accounts. Despite the encryption of card number and bank information, banks cannot process encrypted data and information related to the payments and transactions remain without end-to-end encryption of WhatsApp. [21]

If speaking about Disappearing Messages function, it has many drawbacks that can be abused in certain situations. These are [14]:

- Messages can be deleted only after seven days period and it is not possible to set a timer for self-destruction of certain messages.

- If a user is not using WhatsApp messenger for a week and the Disappearing Messages function is on, messages can still be seen on the notification screen even after deletion

- If certain message is quoted and then deleted, the quote text can still be seen even when initial message is deleted.

- The Disappearing Messages function works only for one chat and it is still possible to forward these messages to another chat with security function off. This way, all forwarded messages will be preserved, even if initial chat was deleted.

- If a certain user creates a backup of the whole conversation before the deletion of messages, then all the data will be preserved.

- It is possible to take screenshots of a chat conversation and there will be no notification. Same with just copying the conversation or taking photos of the device screen.

- By default, all media that user receives through a chat conversation is automatically downloaded to a device that is used at that moment. Even if the security feature is on and all media is deleted after 7 days, some people can still have all this media downloaded.

3.2.5 Privacy Policy

WhatsApp messenger allows its users to use a lot of features and services but for all this to function, a huge amount of data must be collected and processed. For this reason, WhatsApp has its own Privacy Policy to inform users what information is collected as data and how the company uses it. [24]

WhatsApp collects personal information, such as phone number, all messages, media, contact information, logs, location, user presence status, devices and connection, monetary transactions, and all account information. Also, WhatsApp collects cookies to save preferences and some settings. [24]

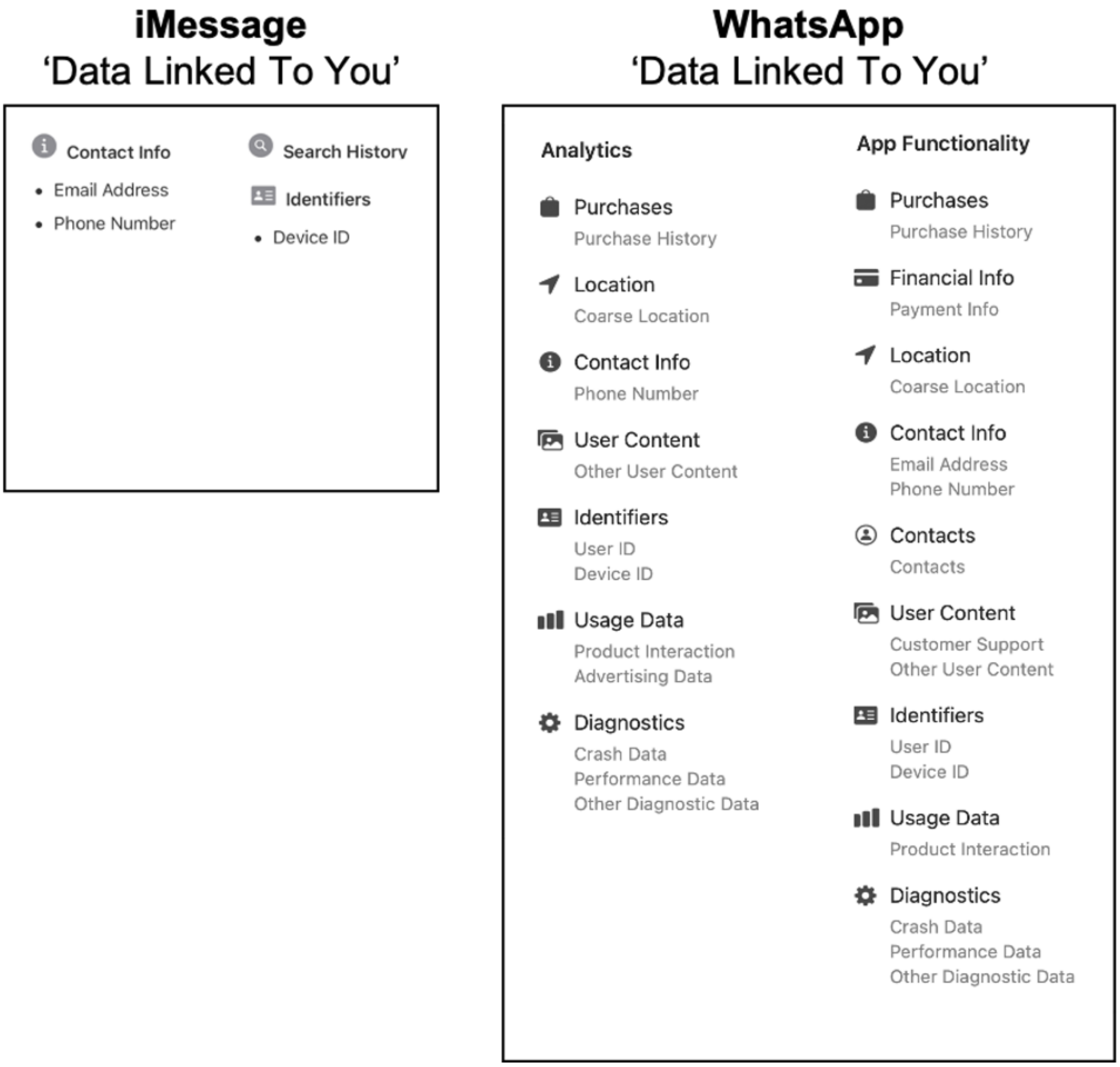
WhatsApp shares personal information with third parties. Privacy Policy states, that when user wants to use some functions of the messenger, some information will be delivered to third parties. For example, if user wants to use Payments feature, he must provide and share his information with banking institutions that WhatsApp is working with. Same with the data backup services and others that are integrated with the messenger application. Furthermore, WhatsApp states that when they share information with third parties, it is only allowed to use this data by the regulations of WhatsApp and the consent of the user. However, Privacy Policy also states that some third parties can collect data directly from the user and use it according to their own policy. [24]

3.2.6 Privacy Policy Issues

WhatsApp Privacy Policy gives the ability for a huge personal data collection that raises some privacy concerns such as: [24]

- WhatsApp shares data with third parties for targeted advertisement
- It is not clear whether the data is used only for the features and as a requirement to use this app or with a purpose of selling it.
- Third parties have possibility to access user data and collect it by different regulations.
- WhatsApp can provide collected data for analytical, educational, or marketing purposes
- It is not clear, whether collected data is anonymous or personalized
- Behavioral data, locations and activity can be transferred to third party companies and it is not stated what are the limits of using this kind of data.
- The consent of user is asked only once, and it is not possible to limit the shared data or to partially deny some statements from the Privacy Policy.

In October of 2020 WhatsApp revealed its plans to merge Business version of the app with Facebook [25]. In January 2021 WhatsApp got a sudden change in its Privacy Policy on Business version of the application. WhatsApp stated that it will be more convenient to use Facebook servers for the business accounts data processing and will merge Business version with its servers on February 8, 2021, giving its users an ultimatum [26]. The users of WhatsApp were already concerned about their privacy because of the amount of data that WhatsApp requests when installing its application. This sudden change only raised more concerns regarding the application privacy [27]. The necessary data for WhatsApp can be seen in comparison with another messenger on the Figure 4. The announcement of new changes can be seen on the Figure 5.



iMessage
'Data Linked To You'

Contact Info
- Email Address
- Phone Number

Search History

Identifiers
- Device ID

WhatsApp
'Data Linked To You'

Analytics

Purchases
Purchase History

Location
Coarse Location

Contact Info
Phone Number

User Content
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction
Advertising Data

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

App Functionality

Purchases
Purchase History

Financial Info
Payment Info

Location
Coarse Location

Contact Info
Email Address
Phone Number

Contacts
Contacts

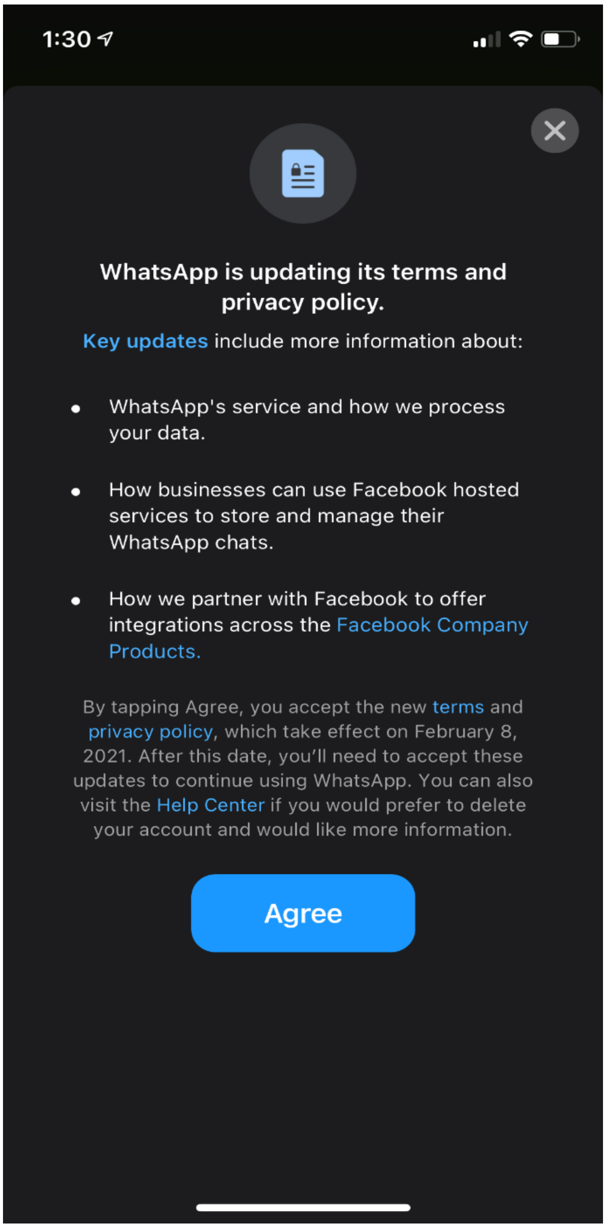
User Content
Customer Support
Other User Content

Identifiers
User ID
Device ID

Usage Data
Product Interaction

Diagnostics
Crash Data
Performance Data
Other Diagnostic Data

Figure 4 Apple 'App Privacy' Labels (Source: https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/?sh=1eb23d303623)



WhatsApp is updating its terms and privacy policy.

Key updates include more information about:

- WhatsApp's service and how we process your data.
- How businesses can use Facebook hosted services to store and manage their WhatsApp chats.
- How we partner with Facebook to offer integrations across the Facebook Company Products.

By tapping Agree, you accept the new terms and privacy policy, which take effect on February 8, 2021. After this date, you'll need to accept these updates to continue using WhatsApp. You can also visit the Help Center if you would prefer to delete your account and would like more information.

Figure 5 The announcement of new changes (Source: https://arstechnica.com/tech-policy/2021/01/whatsapp-users-must-share-their-data-with-facebook-or-stop-using-the-app/)

Because of WhatsApp sudden changes, many users lost their trust in privacy using the app. WhatsApp rivals that provided better privacy policy got a large number of new users that switched to other applications [28]. WhatsApp, faced with such a negative reaction from its users, delayed the Privacy Policy update until 15th of May, 2021 [29].

3.2.7 Privacy Settings and Options

WhatsApp has the most basic and common privacy options. By default, it allows users to see the "last seen" status, basic profile information, profile picture, status updates and everyone is capable of adding a user to any group [30].

In the Options menu it is possible to hide the “last seen” status, profile picture, information about this user, status updates, block invitations to groups and “read” status. When a user hides his “last seen” status he also hides this information for himself about the others. Also, when user disables the “read” status he also cannot see if other users from his conversations have read any message or not. [30]

WhatsApp gives an option of requesting the collected account information. For this feature a request to WhatsApp support is required. [31]

3.2.8 Known Leaks and Vulnerabilities

WhatsApp had several vulnerabilities and some of the most recent and dangerous will be discussed here.

In year 2019 WhatsApp had a serious vulnerability allowing hackers to destroy WhatsApp group chats and client applications. To execute this attack, hackers manipulated the metadata of a message and pasted it into the group chat or conversation. WhatsApp was failing to process this kind of manipulated data and forced the client app to crash without restoration. All users that are in the same group could be affected and have their application killed. To restore WhatsApp application it was needed to reinstall it, but the group itself and all messaging history could not be restored. [32]

WhatsApp was also involved in a spyware scandal. In 2019 WhatsApp had a huge security breach allowing Israeli Spyware to take over the app using just a simple voice call function to install the spyware and steal data or spy on the users. This breach was fixed by an update from WhatsApp. [33]

In February 2020, a new WhatsApp vulnerability was discovered. Despite WhatsApp claiming its high privacy and encryption, it was found that every WhatsApp group was indexing by Google Search. With a specific search of “chat.whatsapp.com” in Google everyone could get a list of groups and an invitation link or see the group’s name. Some groups had very sensitive or private topics and could be seen by anyone. It is possible for group admins to invalidate the invitation links, but it is still possible to find them afterwards. Later, Google somewhat fixed this issue but it is still possible to find some groups that are poorly moderated or set up. [34]

3.3 Facebook Messenger

3.3.1 Description of Facebook Messenger

Facebook Messenger is a messenger application created by Facebook Inc. and was launced in August of 2011. Facebook Messenger has approximately 1,3 billion monthly active users [8]. The application has all necessary and basic functions like sending text messages, making voice calls, design customisation, monetary transactions, share of documents and location etc. [35]

3.3.2 Security Settings and Options

Facebook Messenger has the most basic security options such as :

- Two-Factor Authentication feature that allows to set an additional security code to an account or use a third-party authentication application. It is also possible to add an additional phone number for authentication purposes. [36]

- Login Alerts feature can notify people when someone is trying to log into their account. [37]

- Safer Message Requests feature that will ask permission to accept a message from someone who is not in a user’s friend list. This feature can help in avoiding fake accounts or spam. [38]

- App Lock feature allows a user to have an additional security by setting up a Face ID or fingerprint to unlock chats on a device. [39]

- Secret Conversations is a feature that allows a user to create a secret chat with an end-to-end encryption. With this feature on, a new encrypted chat appears with a function of timer for message self-destruction. However, this will be a new chat and all messages from the unencrypted chat will not be transferred to the new one. [40]

3.3.3 Encryption of Facebook Messenger

Facebook Messenger does not use an encryption by default in the app. However, using a Secret Conversations feature enables an end-to-end encryption. With this feature enabled, only messages, pictures, stickers, videos, and voice recordings are encrypted. Groups, gifs, voice or video calls and payments remain unencrypted. To verify the end-to-end encryption, a device key can be viewed on both ends which must be identical. Private and public keys are unique for every secret chat [41].

3.3.4 Issues of Security Features

Despite having useful security features, there are some issues with security in Facebook Messenger.

Two-Factor Authentication is a very useful feature. However, Facebook messenger will ignore this feature if a user on a new device will use a “Remember Me” option. If a user accidentally will exclude a public device from repeatedly asking verification code, anyone can access this account without two-factor authentication. [36]

Same mistake can happen with Login Alerts feature. If a user will save a browser or a mobile device to a trust list, he will not receive an alert if someone else logged in. [37]

Face ID or fingerprint can also be violated by force of a software error. [23]

Secret Conversations feature is the only option to enable end-to-end encryption. However, this feature encrypts only half the data and demands the creation of a separate chat. Also, it is still possible to make screenshots of this chat and there will be no alerts [41]. Facebook itself stated, that the secret chats are the only function that can be considered encrypted and safe. Default chats are not safe and have the possibility of being leaked. [42]

3.3.5 Privacy Policy

The Privacy Policy of Facebook Messenger is governed by Facebook Inc. and contains information about personal data usage and processing. [43]

Facebook collects the personal information about users, including their behaviour, connection to people, interests and everything that involves your activity in Facebook products. The collected data also includes address books, call logs, SMS logs from the mobile device. Information about financial transactions is also being forwarded to Facebook, including credit card number, bank account details, billing or even delivery information. Facebook receives all metadata, such as time and date of logging in or posting comments and sending or receiving a message and many more. Furthermore, Facebook collects all the information about every device used. This involves the information about device hardware, software, serial number, Wi-Fi connection, Bluetooth, plugins and all applications that are installed, GPS location, camera and photos, all cookies with personal ID, information about other devices that are nearby, phone numbers, IP addresses and the list goes on. [43]

Facebook states, that this information is only used for personalized experience and improvement of all of its products. [43]

3.3.6 Privacy Policy Issues

Facebook's whole Privacy Policy can be considered as an issue. The concerns of users regarding the Privacy Policy started from the beginning of Facebook and throughout the years it has only increased. The main problem of Facebook data collection is that the collected data can be shared with third parties and it is not quite understandable where are the limitations of this data sharing. [44]

The main Privacy Policy issues are:

- All personal information is collected and connected to a particular user. Health, geolocation, behaviour, devices, location, network, identifiers, signals and connections around the device and devices that are nearby, face recognition, interests and purchase information etc. [43]

- Personal information is shared with third parties and can be collected by them independently of Facebook. Third parties have the right to access the collected information and combined with the third party data and verify the identity of user. [43][45]

- Collected data is used for targeted advertisement and marketing purposes even on third party resources and web pages. [43][45]

- Facebook collects even unnecessary cookies of external websites and collects information even when a user does not use Facebook. [43][45]

- It cannot be verified that all collected data share the same confidentiality and integrity on third party servers of how the data is used. [43][45]

3.3.7 Privacy Settings and Options

Facebook Messenger has privacy settings are very general and only involves a user's interaction with other users. The application has the following functions:

- Blocking unwanted users
- Limit the people who can see stories or hide the stories and updates from other people
- Control who can see the active status of a user
- Remove the sent message from the chat
- Clear the search history

3.3.8 Known Leaks and Vulnerabilities

Facebook has a well-known bad reputation and raises concerns of users regarding their privacy and security when using Facebook products. Facebook had many leaks and breaches but the most recent will be discussed here. [46]

In year 2018 Facebook was fined by the UK Information Commissioner's Office for 500,000£ over a Cambridge Analytics scandal. Prior this incident, over the years Facebook gave application developers a nearly unlimited access to user data and had no control over the data usage. Due to this negligence, the data was used for personal gain and the data of almost 87 million users was used to promote political campaigns. [47]

On September 25, 2018 Facebook had a breach which involved data of over 50 million users. Facebook had a vulnerability allowing hackers to exploit "View as" function that allows users to check how others see their page. Hackers stole the tokens that allow to stay signed into a user's account and could take over all the information and messages. [48]

In 2019 Facebook publicly stated, that it has listened to the private voice-to-text audio of the Facebook Messenger users. To test this feature, Facebook used employees instead of software to correct the voice-to-text accuracy without the user consent or knowledge. This claim raised huge concerns of users and gave rise to doubt the importance of privacy for Facebook. [49]

On the April 3rd , 2021 a Twitter user Alon Gal made a post about finding a huge database of Facebook users private information on a hacking forum [50]. This database was shared for free and had personal data on over 533 million user of Facebook that included Facebook IDs, phone numbers, name, birth date, locations, email addresses and more. Facebook stated that this data was leaked in 2019 and the breach has been patched long ago. However, this data can be exploited by anyone and may pose danger to the users which data has been leaked. [51]

3.4 Telegram

3.4.1 Description of Telegram

Telegram is a messaging application that was launched on August 14, 2013 and as stated by the company, it focuses on speed, simplicity, and security. Telegram application is cloud-based and provides a seamless synch for all of its users. Due to synchronisation, it is possible to log in with any device or browser and still have all the chats present which allows more convenience as conversations do not stick to a one device. [52]

Telegram has all the functions of a modern messenger and allows to make calls, exchange unlimited number of files, customize the design, send voice of video messages, create large groups for up to 200,000 people, has multimedia channels and support chat bots and more. [52]

Telegram has an open-source code and API for everybody to check and analyse [52].

3.4.2 Security Settings and Options

Telegram states, that its main goal is to provide privacy and security to its users. Here will be listed all security functions of Telegram. These functions are [52]:

- Two-Factor Authentication allows users to use both an SMS and an additional password to log into the account. It is also possible to set a recovery email address that can help in restoring the access to an account. It is recommended by Telegram to use trusted emails with strong password and a two-factor authentication.

- Secret Chat function allows to make a separate end-to-end encrypted chat with self-destructing messages and a timer. Medea like photos can also be self-destructing and can be viewed only on a device with a secret chat. If someone makes a screenshot, an alert will be sent. It is possible to set a timer even for 1 second and have all messages deleted instantly after they are read.

- Passcode Lock function allows to set up a 4-digit code for accessing Telegram application. Each time a user opens Telegram, it will ask for a code.
- Active Sessions function can show every device that was or is logged in. It is possible to remotely deactivate and account and unlink devices.
- Delete My Account function allows to set a timer for account self-destruction. No restoration is possible after the deletion.

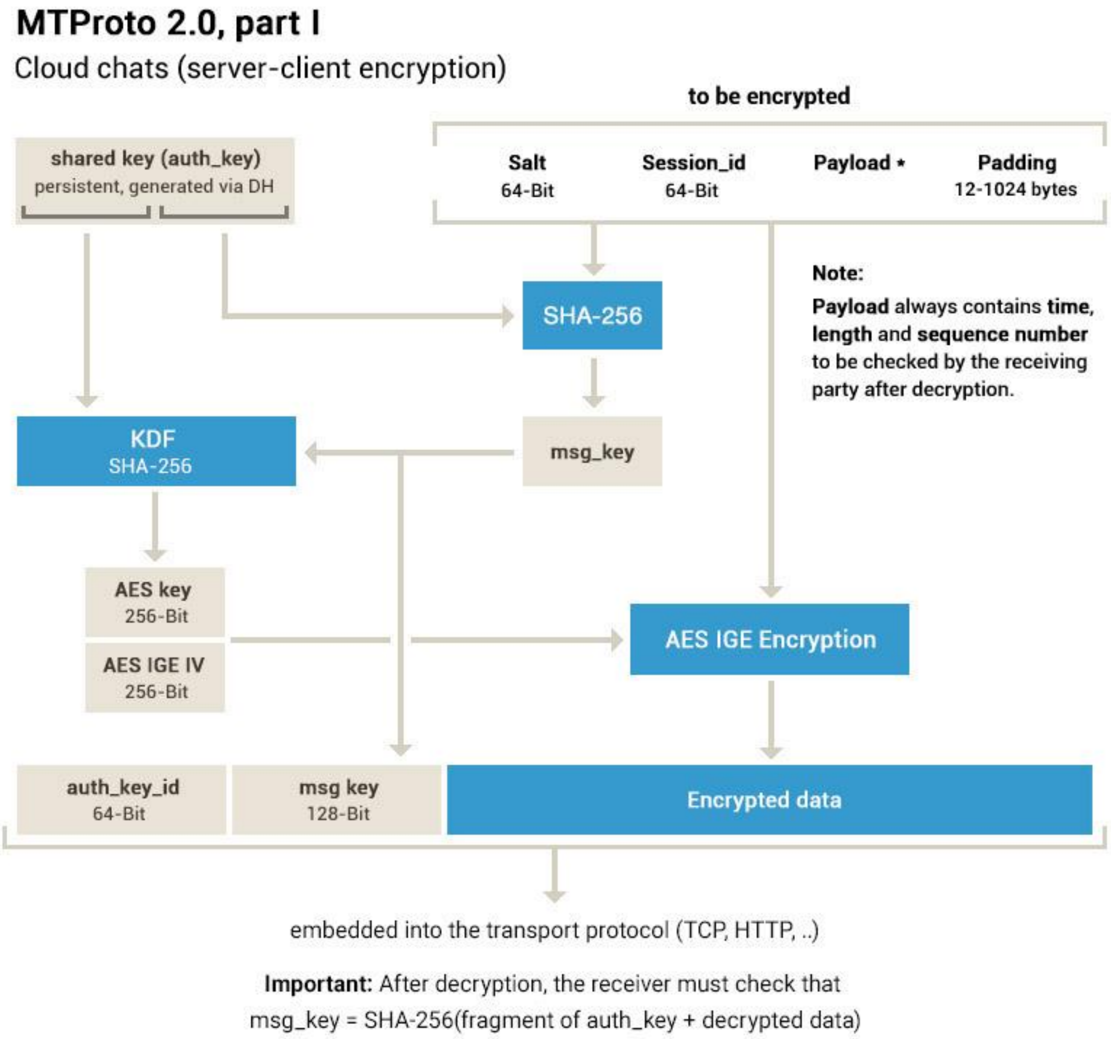
3.4.3 Encryption of Telegram

Telegram is a cloud-based messenger with a support of end-to-end encryption. This way, application supports two kinds of encryption for server-client and client-client.

Telegram uses its own cryptographic protocol MTProto that is designed for both server-client and client-client architectures. This protocol is designed to grant access from a mobile application to a server API [53]. The schemas of both architectures can be seen on Figure 6 and Figure 7

With end-to-end encryption all messages are encrypted for both users and cloud synchronisation in these chats is disabled. To verify end-to-end encryption a special security code can be seen on both sides of the conversation. [54]

On the question “Why not make all the chats with end-to-end encryption?” Telegram states that it values privacy and the speed to the messenger. Having all the chats stored and encrypted on the servers allows users to easy access all their conversations and keep the up to date while having unlimited storage for files or media and saving storage on the device itself. End-to-end encrypted media and messages are stored on the device itself and can be instantly deleted without a trace on the device for both sides. [52]



MTProto 2.0, part I

Cloud chats (server-client encryption)

Note:
Payload always contains **time, length** and **sequence number** to be checked by the receiving party after decryption.

Important: After decryption, the receiver must check that msg_key = SHA-256(fragment of auth_key + decrypted data)

Figure 6 Telegram MTProto 2.0 server-client (Source: https://core.telegram.org/mtproto)

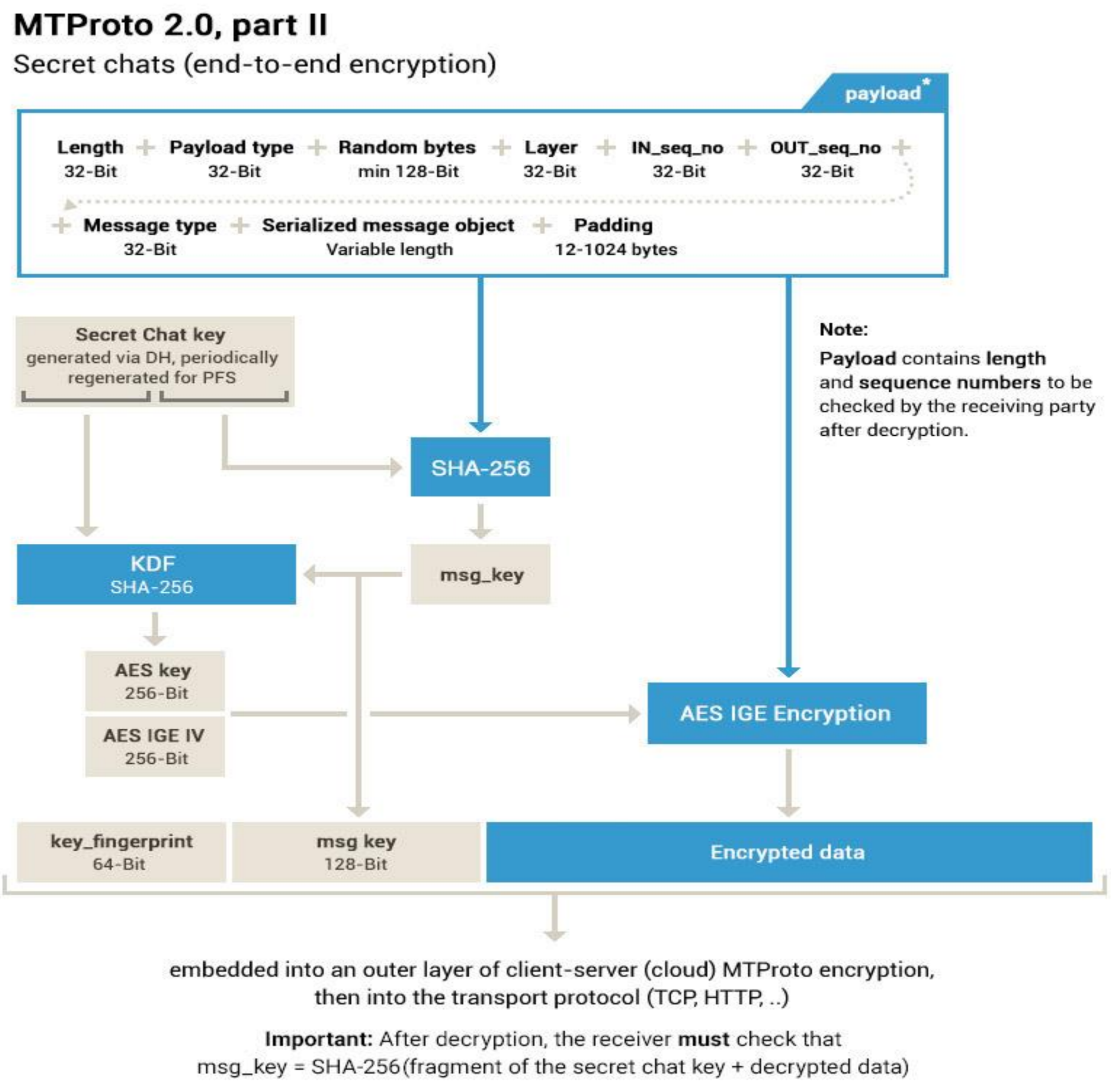

MTProto 2.0, part II
Secret chats (end-to-end encryption)
payload*
Length 32-Bit
Payload type 32-Bit
Random bytes min 128-Bit
Layer 32-Bit
IN_seq_no 32-Bit
OUT_seq_no 32-Bit
Message type 32-Bit
Serialized message object Variable length
Padding 12-1024 bytes
Secret Chat key generated via DH, periodically regenerated for PFS
Note: Payload contains length and sequence numbers to be checked by the receiving party after decryption.
SHA-256
KDF SHA-256
msg_key
AES key 256-Bit
AES IGE IV 256-Bit
AES IGE Encryption
key_fingerprint 64-Bit
msg key 128-Bit
Encrypted data
embedded into an outer layer of client-server (cloud) MTProto encryption, then into the transport protocol (TCP, HTTP, ..)
Important: After decryption, the receiver must check that msg_key = SHA-256(fragment of the secret chat key + decrypted data)

Figure 7 Telegram MTProto 2.0 end-to-end (Source: https://core.telegram.org/api/end-to-end)

3.4.4 Issues of Security Features

Telegram has only few issues with its security features and these are:

- Two-Factor Authentication is overall good, but it is needed from user to have a secure and reliable email address. Otherwise, it is possible to reset the authentication if the email was compromised. [52]

- Secret Chat on Telegram is secure enough, but it still has issues with screenshot notifications. On Android or Windows Phone devices it is still possible to bypass this feature if needed. [52]

- Passcode Lock feature has its limits. It is only possible to enable asking for a passcode for every 5 minutes to 5 hours. If a user stops using his application after less than 5 minutes, it is possible to open the app without the passcode. [55]

3.4.5 Privacy Policy

The Privacy Policy of Telegram is a part of its Terms of Service and describes how data is used and for what purposes.

Telegram states that it has two fundamental principles when the collect the data [56] :

1. Telegram does not use the data for advertisement
2. Telegram collects only the necessary data for the app functionality

The Privacy Policy states that it uses third party services only if a user wants to use payments or some chat bots that are interacting with other software. Telegram requires only phone number and an email if user wants to use it for two-factor authentication and all personal information is stored and transferred only by Telegram servers without the help of third parties. [56]

Telegram also states that all information that is stored on the server or transferred through it is encrypted in transit and is deleted as soon as it is no longer needed. [56]

The information about geolocation is used only if a user enables the feature of locating nearby people who also enabled this function. The location data in deleted as soon as user disables this feature. [56]

3.4.6 Privacy Policy Issues

The Privacy Policy of telegram does not have so many issues. Some of them are [56]:

- Payments use third party services, and it is not clear what kind of data they receive
- Telegram bots are relying on third party. Bots are completely independent, and developers may receive information about user if he will use this function
- Phone number and IP address can be transferred to law enforcements if a court order is issued

3.4.7 Privacy Settings and Options

If talking about Telegram privacy functions, these are [57]:

- Blocking users from viewing or contacting a user
- Hiding phone number or restricting the group of users who can or cannot see it
- Hide “Last Seen/Online” status and profile picture
- Hide the link to a user’s account when his message is being forwarded
- Enable or disable calls
- Restrict others to add a user to a group
- Clear payment and shipping information
- Check if Telegram account is logged into some services and unlink it
- Delete synched contacts and disable this feature
- Enable or disable link previews

3.4.8 Known Leaks and Vulnerabilities

Telegram messenger is secure enough to protect the privacy of its users, however the application still had some vulnerabilities that were exploited recently.

On July 16, 2019, a security vulnerability was discovered allowing hackers to manipulate the media and change the data. This vulnerability exploited the space of time when a photo or a file was downloaded from Telegram to a device and was used by the hackers to manipulate the data. With this attack it was possible to replace media on a device with malicious or fraud file. However, the external storage was an optional for Telegram and only those who enabled it could be affected. [58]

On August 25, 2019, a privacy issue compromised thousands of Chinese users. On a Hong Kong pro-democracy campaigns some people used Telegram as a secure messaging platform to communicate. However, Chinese government found the way to identify these people by their phone numbers, exploiting the contact list and adding thousands of phone numbers to an account. This way, they synched all numbers with Telegram and matched the stored numbers, finding the people that were using it. [59]

On June 24, 2020, Telegram had a database leak of phone numbers for 900 megabytes. Telegram stated that no passwords or messages were present in this leak, only phone numbers and user IDs. To leak the data, the contact import feature was exploited just as it was in Hong Kong. To prevent these kinds of attacks Telegram added the possibility to hide the user’s number from anyone in the options of the application. [60]

3.5 Viber

3.5.1 Description of Viber

Viber is an IM and VoIP application that allows to send messages and make calls or an entire video conference for up to 20 people. Viber has all basic functionality of other messengers and has some unique features like allowing users to put money on their account and making an ordinary cellular call. Also, since Viber focuses on VoIP, great attention is paid to calls and video calls. It is possible to synchronize video calls with several devices and broadcast the video call to another desktop display. [61]

Viber has been launched by Viber Media in year 2011 and was later bought by Japanese company Rakuten for 900 million dollars in year 2014 [62]. Since then, Viber increased its popularity and in May 2020 it had over 1.169 billion registered users [63].

3.5.2 Security Settings and Options

Viber has almost no security settings. All settings are related to privacy and advertisement. The only security feature is the ability to set a password, but only on the desktop version of the application. [64]

3.5.3 Encryption of Viber

Viber uses end-to-end encryption by default in every chat, group chat and voice calls and does not store chats on the server. Primary Viber device uses as an ID a long-term 256-bit Curve25519 key pair for identification and message encryption. Other devices of the same account use PreKeys as a set of medium-term Curve25519 key pairs. For voice calls Viber generates a session ephemeral 256-bit Curve25519 key-pair as a private keys and uses ID keys for public signing. When the call ends session keys are no longer valid.

Private keys are stored on every device separately, while public keys are stored on the server. The chat bots and communities are not end-to-end encrypted but use encryption in transit. [65]

3.5.4 Privacy Policy

The Privacy Policy of Viber is divided into two parts, Viber Privacy Policy and Viber Ads, Cookies & Tracking Technologies Policy [66] [67].

Viber Privacy Policy describes how and what data is collected and how it is used. Viber states, that it collects only the necessary data [66]:

- Registration and account information – phone numbers, name, date of birth and other information that user provides on registration. If a user decides to add information about himself or ling an email, this information will be collected as well.

- Social media information – when a user logs in with Viber on a third-party platform.

- Activity information – when a user makes calls, sends messages, links and other metadata of files and messages without the plaintext.

- Information from other sources like additional contact information.

- Device and location information such as mobile device ID, operating system, hardware, browser, language, wireless networks, IP address etc.

The Privacy Policy also describes the usage of collected data [66]:

- Synchronization of devices – if user decides to synchronize the data and transfer it to another device.

- Provision of customer service – to quickly respond to a report or an issue Viber uses collected information on a specific user.

- Improvement of service – Viber uses call function logs to identify network flow and improve the connection.

- Provision of offerings – Viber may use personal information to notify if a contact from a user’s address book is already present in Viber.

- Process payments and orders.

- Prevent spam and fraud – Viber can analyze the behavior of a specific phone number to analyze if it is suspicious.

- Communication – Viber can use contact information to communicate with users or notify them directly.

- Third parties – Viber can disclose private information to additional service providers or advertisement companies for targeted advertisement. Also, it is stated that if Viber will merge with another company, they can access all the collected data. Law enforcements can request the full data on a user.

Viber Ads, Cookies & Tracking Technologies Policy describes how the application is promoting ads and manages cookies with the usage of personal information [67].

Viber has ads in its application, but users have the ability to limit the data collection by advertisement companies. The partners of Viber - Google Ad Manager, Appnexus, MyTarget, Yandex Mobille Ads, Rakuten Marketing, VK SDK (Connect/Login), Google Analytics, Google Tag Manager, Adjust, Firebase Analytics, Crashlytics, Sentry, Mixpanel, Unbounce, Braze (Appboy), Survey Monkey, Twitter, Google Ads. [67]

3.5.5 Privacy Policy Issues

On the topic of privacy policy issues, Viber has similarities with Facebook Messenger as it is collecting data for marketing purposes. However, user still has some control over some data that is being used for advertisement. [66]

The main issues of Viber are [66]:

- Viber has the ability to disclose the data to its partners and show ads inside the application

- Viber has the ability to collect the data about devices, browsers and connections

- Viber and its partners can use cookies for targeting purposes

- Viber can collect information about the links that a user opens while using the app
- Personal information can be viewed and collected by third parties

3.5.6 Privacy Settings and Options

When talking about privacy settings of Viber, it has many functions to limit the data collection or hide information from others. The privacy features were analyzed by the author using the Viber version 15.1.0.3. on an Android device.

Some of these functions are:

- Basic functions – hide ’online’ status, ’last seen’ status, photo, birth date, allow friend suggestions and trusted contacts, control how can add a user to a group
- Hidden chats – it is possible to hide a particular conversation and set up a passcode to open it.
- Peer-to-peer – this function allows to use peer-to-peer on calls but this feature completely reveals a user’s IP address
- Personal data restrictions – user can disable the collection of analytics data, disable personalized ads, disable interest-based ads, hide accurate location data.
- Ad preferences – user can disable personalization based on links or third-party data, refuse to store cookies and/or access information on a device, disable personalized ads and content profile, prohibit the collection of ad performance records, market research and improvement of product, collect device characteristics for ad purposes etc.

Viber has over a hundred clauses in its Ad preferences and user can manually enable or disable each vendor or ad personalization settings.

3.5.7 Known Leaks and Vulnerabilities

In terms of Viber, are not so many leaks or vulnerabilities found recently. The most recent incident was in Nepal on 16 of April 2020 when attackers tried to catch many users on the binding of a new device. When a new device is connected to the Viber account, an SMS comes with a confirmation and a link. If the user accidentally clicks on the link, then an automatic login from another device will occur and the attacker will gain access to the account. But this vulnerability is based only on social engineering and user carelessness. [68]

3.6 Signal

3.6.1 Description of Signal

Signal is an open-source and nonprofit IM application that focuses on security and privacy of its users. Signal was founded by a cryptographer and computer security researcher with a pseudonym “Moxie Marlinspike” in 2014. In year 2018 one of the WhatsApp founders Brian Acton invested in Signal 50 million dollars and gave it a boost for development [69]. On January 12, 2021 Signal reached over 50 million installations in Google Play [70].

Signal has all the necessary IM functions, such as messaging, voice calls, video calls, groups, design customization, payments, broadcast media etc. [71]

3.6.2 Security Settings and Options

Signal is based on the idea and the privacy and security of its users. Here are the security features that Signal allows users to set up [71]:

- Two-Factor Authentication or PIN – this feature is not the same that is present in most messengers. Signal sets a PIN code by default on the installation of the application. It is possible to deactivate the PIN code but upon re-registration there will be no data on a new device. Even if someone tries to log into the account from another device, it is not possible to get the messages.

- Screen Lock – an additional lock with timer for the application on a particular device.

- Screen Security – fully disables screenshots inside the application.

- Incognito Keyboard – requests keyboard to disable personalized learning or tracking.

- Relay Calls – relays all calls through the Signal server and hides the IP address of a user.

- Link Previews – ability to disable link previews for the chat.

- Registration Lock – every time a new device is linked, Signal will ask a PIN code. Without it, it will be not possible to link a new device.

- PIN Reminders – the application automatically reminds the users to re-enter the PIN code to remember it more quickly.

3.6.3 Encryption of Signal

Signal uses end-to-end encryption by default on all devices and chats. All messages and media are encrypted by the same Signal Protocol [72].

Signal Protocol uses [72]:

- EdDSA signatures with public and private keys for the X25519 and X448 elliptic curve Diffie-Hellman functions.

- Extended Triple Diffie-Hellman key protocol to establish a shared secret key between users.

- Double Ratchet algorithm to exchange messages with a shared secret key.

- Sesame algorithm to allow encryption on a multi-device scenario.

3.6.4 Issues of Security Features

The signal has good security features, but some are not as good as others. For example:

- Screen Security could be a good feature, but it only disables the screenshots on a particular device and not for the both participants [73].

- Incognito Keyboard feature can only send a request to an operating system to disable personalized learning but it does not guarantee that keyboard would not just ignore it [74].

3.6.5 Privacy Policy

Signal states that they use the best encryption methods and their customer privacy comes first. The information that Signal collects and how it is used is described in the Privacy Policy of Signal. [75]

Signal states that it collects only the necessary information, such as [75]:

- Account information – phone number that was used for registration, profile picture, name. Signal uses this information only to connect users.
- Messages – private keys are stored only on a user device and cannot be accessed by Signal. Messages are only relayed through the server fully encrypted. Signal may store messages for a short period of time is a user is out of the network and cannot receive the messages.
- Contacts – Signal can import and discover which contacts are already using Signal. However, this function is optional, and user can deny the access to the address book.
- User Support – Signal may collect the necessary information that a user provides when writing a report to the support team. The messages are deleted as soon as the problem is solved.

Privacy Policy also describes the relationship of Signal with third parties. For example, Signal uses a third-party providers to send verification codes to a phone number. These third parties are using their own privacy policies [75].

Signal can also share information if [75]:

- Law enforcements request it.
- User violates the rules of Signal.
- A user is spreading spam or fraud.
- Safety of other users is at risk.

3.6.6 Privacy Policy Issues

The Privacy Policy of Signal is very short and there are not so many issues with the Signal statements. However, it is not described which third-party services are collecting information and what are their policies [75].

3.6.7 Privacy Settings and Options

The Signal has the most basic privacy features that are present in all messengers. The privacy settings are [76]:

- Hide 'Read' status of a message and 'Typing' indicators.
- Hide the 'Online Status' and disable messages from people that are not in the contact list.
- User can choose not to import his contacts to the Signal.
- User can easily unregister his phone number or delete his account and all chats with one click.

3.6.8 Known Leaks and Vulnerabilities

Despite the fact that Signal focuses exclusively on protection and privacy, a vulnerability was also discovered. In 2019, a vulnerability in the messenger allowed hackers to eavesdrop and spy on the user. The vulnerability worked only on Android and allowed making a call and then initiating an autoreply without the user's knowledge. However, in order to carry out this attack, it was necessary to bypass the security code of the application and change the parameters, which makes this attack difficult to execute and not aimed at the general user. Subsequently, the vulnerability was fixed. [77]

3.7 Discord

3.7.1 Description of Discord

Discord is a proprietary free messenger with support of VoIP and video conferencing, designed for use by various communities of interest, most popular among gamers and students and has over 100 million monthly active users. Discord was launched by Jason Citron and Stan Vishnevskiy in year 2015. The founders of Discord stated that they wanted to create a platform where people can communicate, share their experience and have fun. The application has many functionalities, such as messaging, calling, video calling, creating large groups and whole communities and has many possibilities for customization of groups. For large groups there is also a paid subscription called Discord Nitro to further increase the bandwidth, quality of streaming or video calls, personalize profiles and allow the transmission of files more than 100MB. [78]

3.7.2 Security Settings and Options

Discord does not have many security features. Only the two-step verification and a password that the user sets during registration are available. Two-step verification uses third-party code generation apps such as Google Authenticator or Authy. Also, a user can additionally bind his phone to be able to receive codes by SMS. If the user is not able to obtain the codes by the methods described earlier, Discord provides additional codes to restore access to the account, which the user must memorize and write down for himself. Same authentication method can be used by group administrators to secure their communities. [79]

3.7.3 Encryption of Discord

Discord does not have end-to-end encryption and only encrypts data in transit with HTTPS protocol [80].

3.7.4 Privacy Policy

Discord also collects user data and processes it to provide the functionality. The data that Discord collects and how it is used [81]:

- Discord collects all the data that the user provides, such as email, phone, all messages, media, data on voice calls and video calls.
- Discord automatically collects IP address, device ID, and activities of users.
- Demographics, interests, and behavior of users is collected and can be analyzed. Discord can share this data with its third-party partners.
- With a permission of a user, Discord can collect information from social networks and merge this data with already know data from Discord.

- Cookies are collected to keep track on local computer preferences or to promote ads.

- Discord is integrated with Facebook, Twitter and other services and can provide information to these companies for advertisement purposes.

- Discord does not respond to “Do Not Track” signals and ignores them.

Discord can disclose personal information [81]:

- It is needed for customer service

- It is needed for marketing purposes, such as using email to promote new features of Discord.

- If there is a request by law enforcements

- For the developers using Discord SDK or API the data of end user is always fully available, including message content, message metadata, and voice metadata.

- Discord can provide personal information to consultants, agents or other third parties that Discord hires.

3.7.5 Privacy Policy Issues

As it can be seen Discord collects a lot of data about its users which causes these issues [81]:

- Discord states, that developers can see all messages of groups and users in plain text. This is a huge disadvantage and poses a potential risk to user privacy.

- Discord cooperates with companies such as Twitter and Facebook and may transfer personal data to them.

- Discord uses personal data for targeted advertisement if the user does not uncheck the box in the settings.

- Discord claims that the user should be careful with what information he himself transfers to the service.

In the Terms of Service Discord states “By uploading, distributing, transmitting or otherwise using Your Content with the Service, you grant to us a perpetual, nonexclusive, transferable, royalty-free, sublicensable, and worldwide license to use, host, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform, and display Your Content in connection with operating and providing the Service.” [82]

3.7.6 Privacy Settings and Options

Discord provides some control over the data that the user transfers to the server and who can communicate with it. There are functions like [83][79]:

- Disable sharing data to improve Discord.
- Refuse to personalize the data.
- Turn off statistical data collection.
- Remove sychronized services and connections.
- Safe Direct Messages – allowes discord to scan messages for explicit content or messages and automatically block them.
- Hiding ’Online’ status or block friend requests from strangers.

3.7.7 Known Leaks and Vulnerabilities

Despite the fact that the discord had almost no data leaks, there were cases of virus infection.

In year 2020 Discord could be infected with AnarchyGrabber that modified the JavaScript code of the Discord client and launches the virus with Discord application, stealing passwords of users [84].

The most recent attack was in April 2021. Attackers used Discord to embed a ransomware, cryptocurrency mining malware or spyware into the links, hiding them under the disguise of videos or photographs. When a user clicked on these links, a malicious code could be installed on their client. It was also possible to use Discord clients as command-and-control elements to harvest and steal data in the same way as the botnet do. Discord allows to use clients as a ‘webhook’ and automatically update and pull information from sites and groups. Cybercriminals used this feature to relay stolen information from compromised clients directly to cybercriminal servers. [85]

Recently, Discord was accused of censorship, due to the blocking of groups dedicated to those interests that are not close to Discord or do not correspond to its views. [86][87]

3.8 Snapchat

3.8.1 Description of Snapchat

Snapchat is a proprietary IM application with the core concept that the transmitted images and messages are only available to the recipient for a short time before becoming completely inaccessible [88]. Snapchat has over 498 millions of monthly active users and is more popular with teens and millennials [8][89]. Snapchat specializes in sending photos that can be set to a self-destruct timer. There is a huge number of different masks, filters, and effects to create variety of original photos. There is a "Stories" function in Snapchat, where the user can upload various short videos or photos that will disappear after 24 hours. [90]

3.8.2 Security Settings and Options

Snapchat does not have many security features. The main feature is two-factor verification with a third-party authentication app like Google Authenticator or Duo. It is possible to create Recovery Codes just like in Discord, so if a user loses access to his authentication app, it is possible to use a recovery code. [91]

3.8.3 Encryption of Snapchat

Snapchat has end-to-end encryption by default but only for snaps. All the messages and group chats or calls are not end-to-end encrypted. It is not known if Snapchat uses encryption on its servers. [92]

3.8.4 Privacy Policy

Snapchat is one of many applications of Snap Inc. and is governed by the Snap Inc. Privacy Policy and regulations. [93]

Snap Inc. collects and uses [93]:

- Information provided by user, such as all the messages, photos, stories etc.
- Collected information – all activity of user, such as what filters are used, all metadata of photos and other media, every interaction with the application and logs, custom made stickers or images.
- Information about the device - hardware and software, hardware model, operating system, browser, applications, advertising identifiers, battery, unique device and app identifiers, which devices are connected, information about accelerometers and gyroscopes, microphone, Wi-Fi and other network connections, IP addresses.
- Device phonebook and all contacts with the permission of user.
- Information about camera and photos.
- Precise location information, GPS, networks around the device, cell towers, sensors etc.
- Cookies for marketing purposes.

Snapchat has the possibility to collect and share information with third parties for targeted advertisement or to personalize the experience for each user. However, it is possible to limit the information collected through Snapchat Options. [93]

3.8.5 Privacy Policy Issues

The Privacy Policy of Snapchat has similarities with Facebook Messenger, as it is collecting too much information and uses it for advertisement purposes.

3.8.6 Privacy Settings and Options

Despite the fact that Snapchat uses data to promote ads, it contains settings that can limit the collection of data. For example [94]:

- It is possible to turn off audience-based ads, activity-based ads, third-party ad networks.

- User can turn off personalization of content, such as categorization by lifestyle, tags, activity etc.

Also, Snapchat has the most basic privacy settings, such as [95]:

- Hiding who can see stories, location, profile information.
- Blocking contacts or notifications from users
- Creating a private stories or snaps

3.8.7 Known Leaks and Vulnerabilities

Snapchat did not have leaks or vulnerabilities found recently. However, there were cases of illegal use of data and stalking.

In May 2019, a violation was identified in which a Snapchat employee illegally used a tool called SnapLion that collects user data for law enforcements to achieve his personal gain and harvest data. [96]

In 2017 a feature called Snap Map raised privacy concerns of Snapchat users. This feature allowed to show your real-time location on a map inside Snapchat application and all users from a friend list could trace the precise location and the address. If a stranger adds a user to his friend list it is also possible for him to trace and stalk on people. [97]

3.9 WeChat

3.9.1 Description of WeChat

WeChat social network was developed by the Chinese tech giant Tencent. The company has risen on the QQ instant messaging service, which dominated the home market in 2011. When WeChat was launched, its explosive growth was driven by the relocation of the user base from QQ. It is now very popular because the main competitors such as WhatsApp, Instagram, Facebook Messenger and Telegram are blocked in China. [98][99]

If a user tries to register, he will need another person registered at least six months ago to send an invitation [100]. Furthermore, outside of China, Tencent only supports the basic functionality of the messenger, while in China it has the functionality of an entire ecosystem [98].

WeChat in China can be a translator, a map, a food delivery and a shop application, a bank, a newspaper, a gaming platform, a perosnal document [101].

3.9.2 Security and Privacy Options

WeChat does not have adequate security settings except the registration process. Also, WeChat does not have any useful privacy settings. While being the most popular messenger in China, the messenger itself does not provide its users with the most needed privacy or security options. WeChat does not use end-to-end encryption and only has symmetric AES encryption in transit [102].

3.9.3 Privacy Policy

WeChat Privacy Policy describes which data is collected and how it is used. WeChat collects such data as [103]:

- Registration data, login data, user profile search data, profile data and media, chat data, messages, contact list, locations, personal identifiers, metadata of all content, cookies, social connects

- Additional Account Security data – email, voiceprint, contacts, managed devices, Facebook connect OpenID, Facebook connect tokens, Facebook username and info, credit cards, facial mapping, AppleID etc.

- Every interaction with additional services is logged and saved.

3.9.4 Privacy Policy Issues

WeChat is not a completely private platform and is free to share data with third parties and employees. Also, messages transmitted via WeChat are not end-to-end encrypted and are available in open form for censorship and analysis. [102][103]

3.9.5 Known Leaks and Vulnerabilities

The main problem with WeChat is total censorship and transparency of data without strong encryption of user data. WeChat offers a very wide range of services and does not worry about the data of its users at all [104].

In March 2019 there was a data leak that left over 364 million records online. The data contained personal and sensitive information, such as what are the preferences of the user or history of geolocation. [105]

WeChat has censorship embedded on its servers. Messages are not encrypted for a reason; in China, all messages are analyzed on the server and censored. If a user tries to write something that discredits the ruling party of China, this message will not be delivered to another user, and a notification will be sent to the person who wrote this message that such writing is prohibited. [106]

On February 2, 2021 Tencent executive Zhang Feng was under investigation for alleged corruption and WeChat data sale to former Vice Public Security Minister Sun Lijun [107].

3.10 Jabber

3.10.1 Description of Jabber

Jabber is an open-source IM project based on XMPP (Extensible Messaging and Presence Protocol). Jabber is not an application, and it is possible to use a variety of other clients, such as Adium, ChatSecure, Conversations, Gajim, Jitsi, Messages, Pidgin, Psi, or Swift and be interconnected. XMPP is a completely open protocol, and no one owns it. It is possible to create clients based on the needs and connect it to the network. [108]

3.10.2 Security of Jabber

The privacy and security features depend on the variety of clients and can be very different. If a client supports end-to-end encryption, the messages will be encrypted and vice-versa [108]. Also, XMPP protocol allows to create networks in isolation from the Internet and increase the security even further. XMPP can be used not only for IM but also for file sharing, management, cloud computing, gaming, web services etc. [109]

3.10.3 Privacy Policy of Jabber.org Service

Jabber.org is one of many XMPP services that connects different clients together. As every service or application, Jabber.org has its own Privacy Policy. [108]

Jabber.org states, that it does not store any information, except passwords, logins, or information that user himself reveals to public. Transport Layer Security and Secure

Sockets Layer protocols are used for encryption in transit and Jabber.org uses protected hosting servers with restricted physical access. [110]

Privacy Policy also states that the user should consider that privacy also depends on the application and it may have its own privacy policy [110].

4 Analysis and Results

4.1 Comparison of Described Messengers

As it can be seen, messengers can be very similar or very different, in this part of the study, a table will be compiled based on the theoretical part, according to which it will be possible to show the functions of messengers and clearly demonstrate their differences in the terms of security and privacy. The comparison can be seen in the Table 1.

Table 1 Comparison of Security and Privacy Features

Security and Privacy	**WhatsApp**	**Fb Messenger**	**Telegram**	**Viber**	**Signal**	**Discord**	**Snapchat**	**WeChat**	**Jabber**
End-to-end encryption	YES	Optional	Optional	YES	YES	NO	Only photos	NO	Depends on client
Lock or password	YES	YES	YES	On PC	YES	YES	NO	NO	Depends on client
2-Step Verification	YES	YES	YES	NO	YES	YES	YES	NO	Depends on client
Open source	NO	NO	YES	NO	YES	NO	NO	NO	YES
List of connected devices and remote deactivation	YES	YES	YES	YES	YES	NO	YES	NO	Depends on client
End-to-end encrypted by default	YES	NO	NO	YES	YES	NO	NO	NO	Encrypted in transition
Proxy	NO	NO	YES	YES	YES	YES	NO	NO	Depends on client
Messages stored on servers	NO	YES	YES strong encrypt.	NO	NO	YES	30 days	YES	Depends on client

Security and Privacy	WhatsApp	Fb Messenger	Telegram	Viber	Signal	Discord	Snapchat	WeChat	Jabber
Screenshot alert	NO	NO	YES (iOS works better)	NO	Only on the device	NO	NO	NO	Depends on client
Deletion of messages for both sides	YES	YES, but all users are notified	YES	YES	YES	YES	It is possible to save	NO	Depends on client
End-to-end encrypted calls	YES	NO	YES	YES	YES	NO	NO	NO	Depends on client
Targeted advertisement	YES	YES	NO	YES	NO	YES	YES	YES	NO
Third-party data collection	YES	YES	Only if using bots or payments	YES	NO	YES	YES	YES	Depends on client
Censorship	NO	NO	NO	NO	NO	Partially	NO	YES	NO
Collected data can identify the user	YES	YES	NO	YES	NO	YES	YES	YES	Depends on client
Data can be viewed in plain text	NO	YES	NO	NO	NO	YES	YES	YES	Depends on client
Too much data collected (hardware, connections, devices, health etc.)	YES	YES	NO	YES	NO	YES	YES	YES	Depends on client
Possibility to limit advertisement data share	NO	NO	No ads	YES	No ads	YES	YES	NO	Depends on client
Safety priority	NO	NO	YES	NO	YES	NO	NO	NO	YES
Critical leaks	YES	YES	Only phone numbers	NO	NO	YES	YES	YES	NO

This table was compiled by the author on the basis of all the collected data, which can be found in the theoretical part or by links to sources. Also, the opinion of focus group was taken into account.

If to consider all the most necessary and useful functions, as well as the privacy policy, then the most promising messengers will be: Signal and Telegram. Jabber is also a unique platform for creating highly secure chats and, if properly configured and used, can be the most secure of all.

Not bad, but not the safest messenger is Viber. Despite not having a large list of security features and having advertisement, Viber has a very detailed privacy settings that allow user to manually disable all advertisers or targeting, as well as read the privacy policy of other companies with which Viber works. There are more than a hundred such checkboxes.

Discord and Snapchat are specialized messengers that target a specific audience. Consumers are satisfied and these services have never positioned themselves as secure and do not plan to introduce new technologies or improve encryption. However, this does not negate the fact that these services lack security and privacy.

Some of the most insecure messengers are WeChat, Facebook Messenger, and WhatsApp, which have many data leaks and public scandals on their account. It may seem that WhatsApp is safer and more reliable than Facebook, however, Facebook still owns it, and the latest news show that WhatsApp is increasingly integrating into Facebook services, which have a colossal collection of data and a negligent attitude towards it.

4.2 Survey Analysis

4.2.1 Results of the Survey

In order to analyze messengers, it was decided not only to consider their actual aspects, but also to conduct a survey and find out people's opinions on the topic of security and privacy, as well as their preferences in the functionality of messengers.

The questionnaire had 25 questions and, as a result, it was possible to collect 46 answers. All people interviewed were employees of the company where the author had an internship.

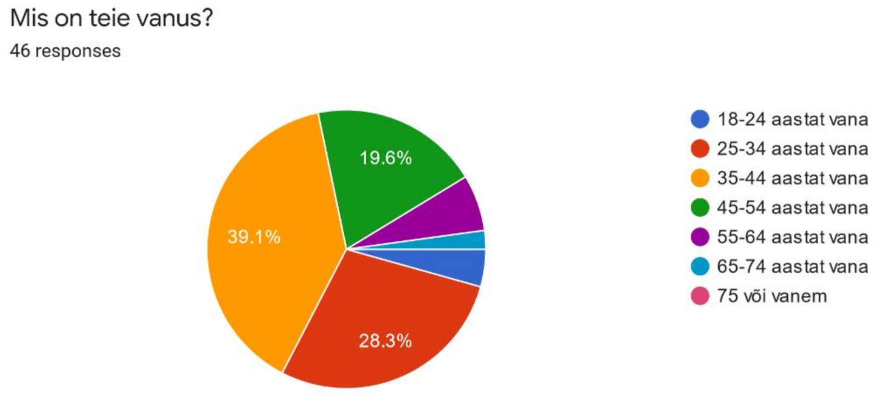


Figure 8 Survey question 1

The first question was the age group of the respondents. People between 18 and 24 were 4.3%, between 25 and 34 – 28.3%, between 35 and 44 – 39.1%, between 45 and 54 – 19.6%, between 55 and 64 – 6.5%, between 65 and 74 – 2.2% and there were no 75 or older respondents. The graph can be seen on the Figure 8.

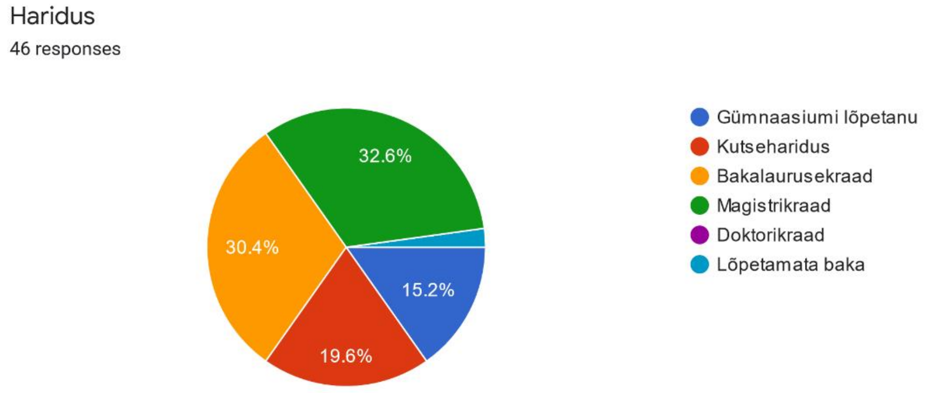


Figure 9 Survey question 2

The second question asked about the education level of respondents. 15.2% were high school graduates, 19.6% were vocational education, 30.4% had bachelor’s degree, 32.6% had master’s degree and 2.2% had ungraduated bachelor’s degree. The graph can be seen on the Figure 9.

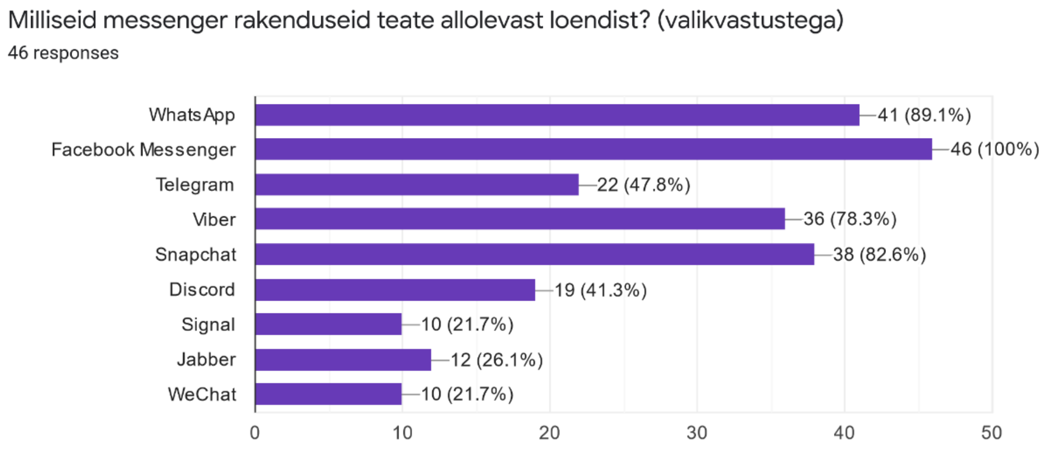


Figure 10 Survey question 3

The next question asked about the messengers that respondents know. The most famous were WatsApp and Facebook Messenger with 89.1% and 100% of those who heard. Viber and Snapchat had 78.3% and 82.6%. About Telegram and discord knew 47.8% and 41.3% of respondents. The most unknown to people turned out to be Signal with 21.7%, Jabber with 26.1% and WeChat with 21.7% of respondents. The graph can be seen on the Figure 10.

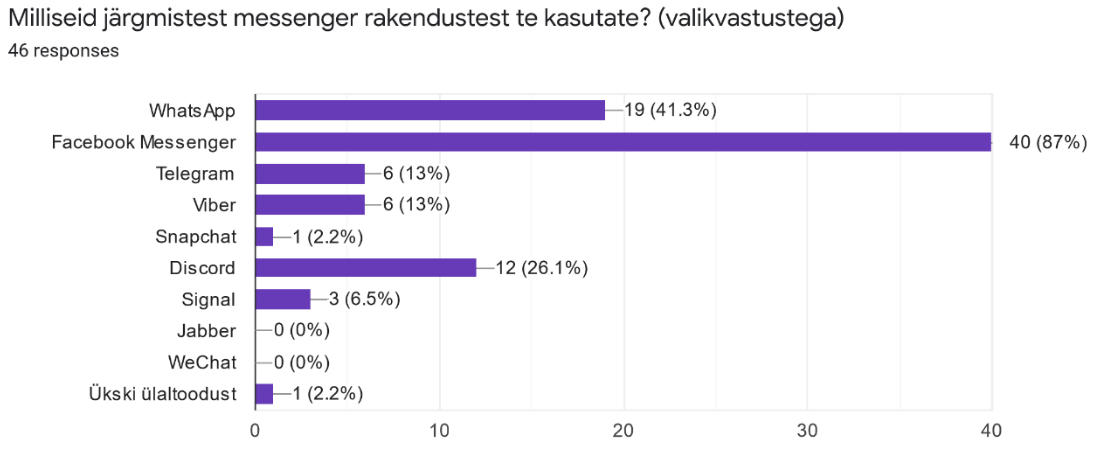


Figure 11 Survey question 4

Here respondents were asked about which messengers they use from the list below. The most popular was Facebook Messenger with 87% of respondents. WhatsApp had 41.3%

of users and Discord is used by 26.1% of respondents. Telegram and Viber had only 13% of users, while Snapchat and Signal had only 2.2% and 6.5% of users. One of the respondents does not use any of those messengers. Nobody uses Jabber and WeChat. The graph can be seen on the Figure 11.

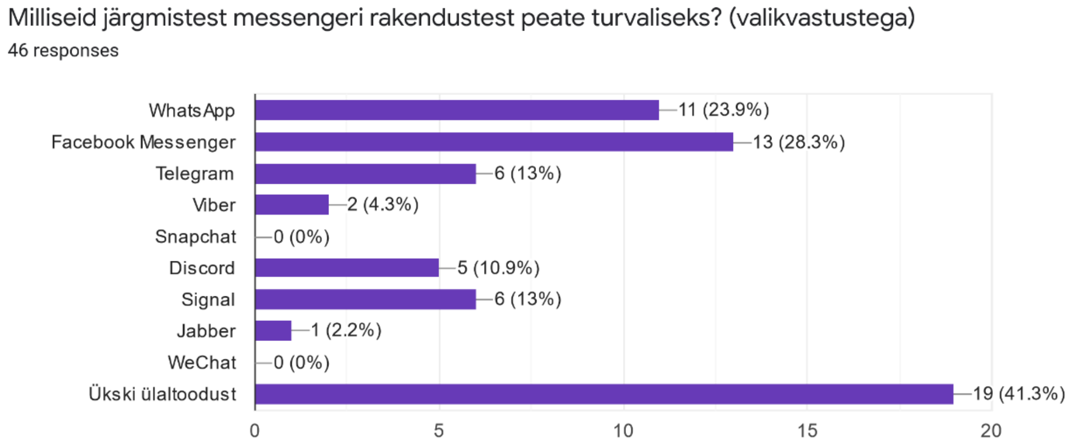


Figure 12 Survey question 5

Respondents were asked which messenger they consider secure. 23.9% think that WhatsApp is secure, 28.3% think that Facebook Messenger is secure, 13% and 4.3% think that Telegram and Viber are secure, Discord had 10.9% and Signal had 13% of respondents. Snapchat and WeChat had 0%. 41.3% of respondents think that these are not secure messengers. The graph can be seen on the Figure 12.

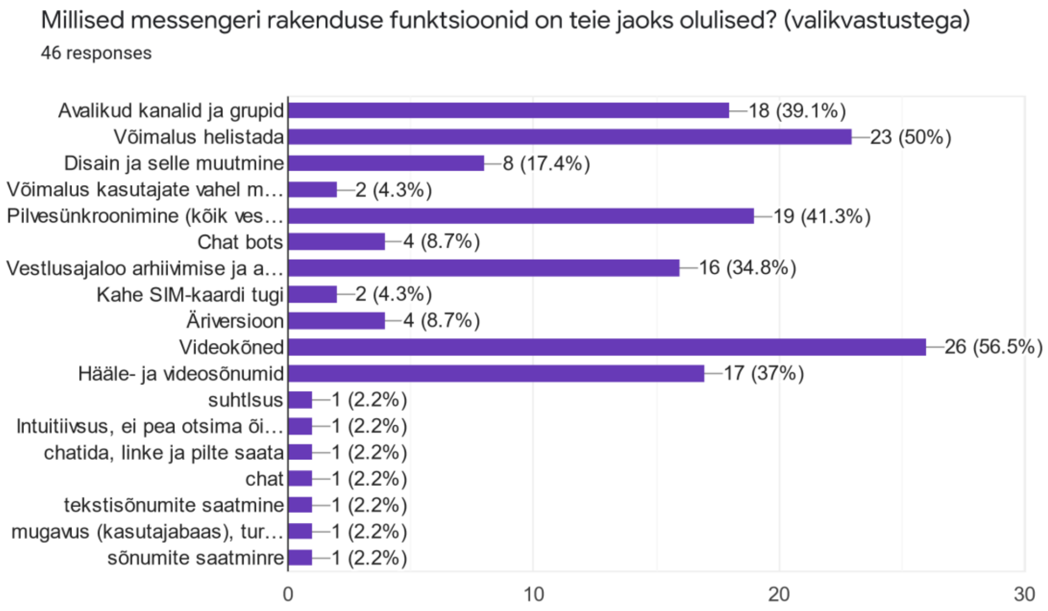


Figure 13 Survey question 6

This question asked what common functions in messengers are important to people. For 39.1% of people, channels and groups are important, for 50% of all respondents, calls are important. For 17.4%, design and customization are important. Only 4.3% think that payments are important, 41.3% of respondents want to have cloud synchronization, 8.7% want to have chat bots, 34.8% think that chat archive export is important, 4.3% of people want support for dual sim cards, 8.7% want to have Business version of an app, 56.5% want to have video calls and 37% want to have audio and video messages. Some respondents also wanted to have easy to use interface and convenience, but this is covered in other question. The graph can be seen on the Figure 13.

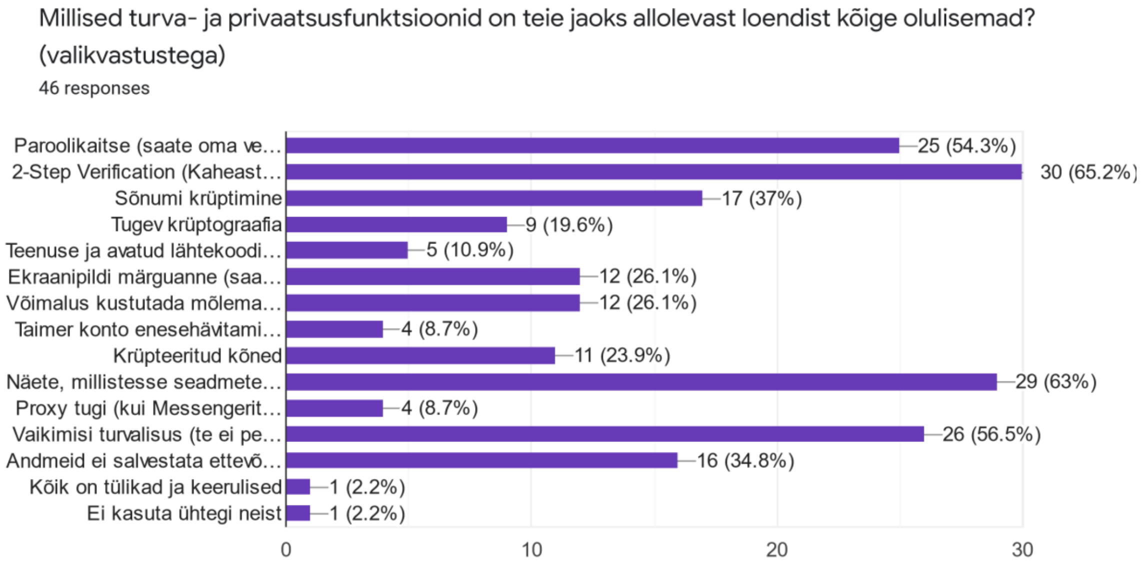


Figure 14 Survey question 7

Here the question was about the most valued security and privacy features. The most popular features were: Device unlinking and 2-Step Verification with 63% and 65.2% of respondents. Also, the popular ones were password protection with 54.3% and protection by default 56.5%. Encryption had 37% and no data on the company servers had 34.8%. 19.6% wanted strong cryptography, 10.9% want an open-source application, 26.1% of people wanted to have screenshot alert and the ability to delete messages, 8.7% want timer for message self-destruction. 23.9% of respondents value encrypted calls, 8.7% want the Proxy support. 1 respondent responded that these features are too complex and the other one does not use them at all. The graph can be seen on the Figure 14.

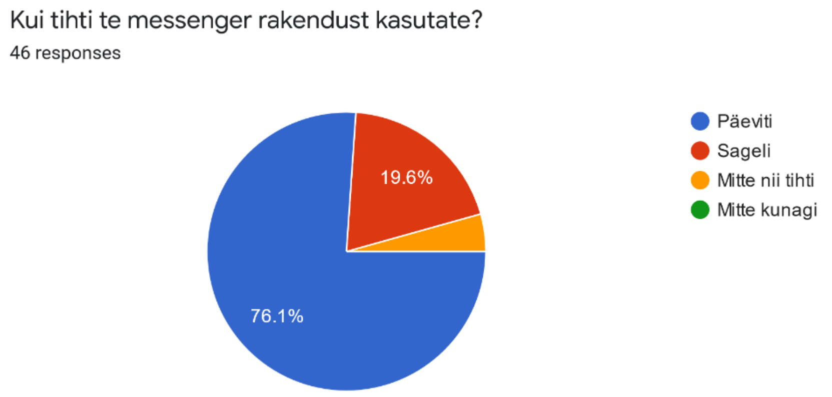


Figure 15 Survey question 8

The respondents were asked, how often do they use a messenger application. 76.1% use it daily, 19.6% use it seldom and 4.3% rarely use it. The graph can be seen on the Figure 15.

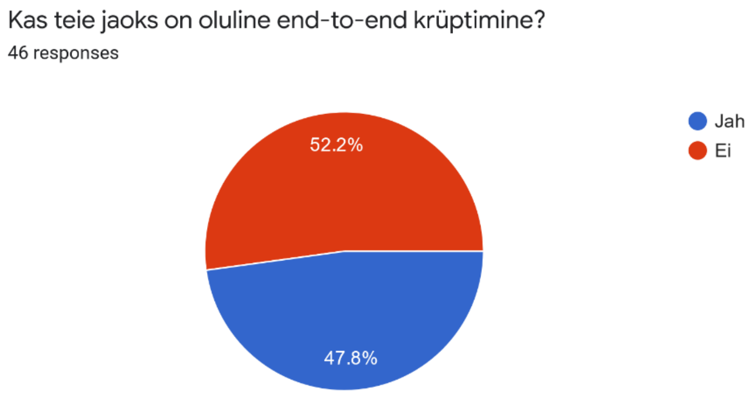


Figure 16 Survey question 9

The respondents were asked, how much do they value end-to-end encryption. 52.2% do not need it and 47.8% do need end-to-end encryption. The graph can be seen on the Figure 16.

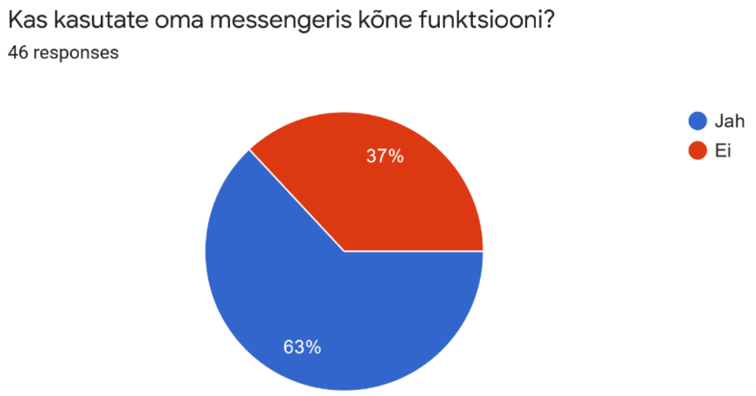


Figure 17 Survey question 10

Do respondents use the call function? 37% do not use, 63% use it. The graph can be seen on the Figure 17.

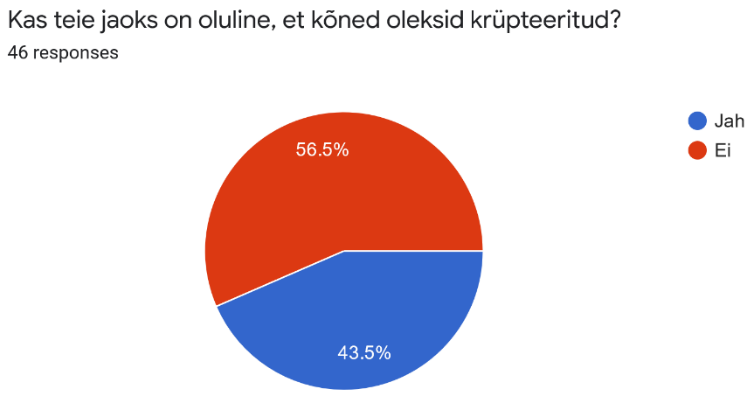


Figure 18 Survey question 11

Do respondents need the voice call encryption? 56.5 do not need it, 43.5% do need the encryption. The graph can be seen on the Figure 18.

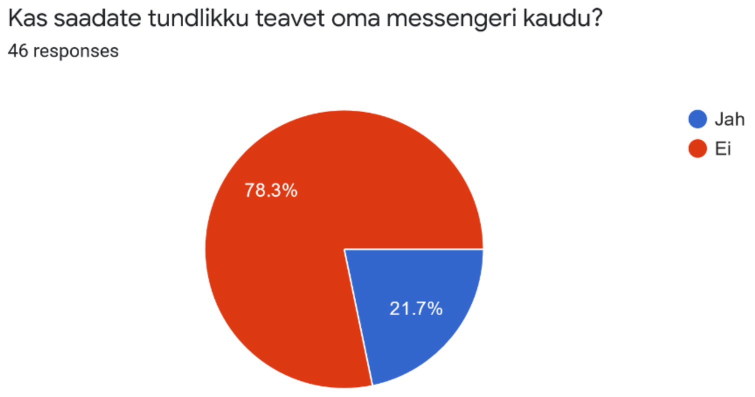


Figure 19 Survey question 12

Do respondents send sensitive information through the messenger app? 78.3% do not send sensitive information, while 21.7% send. The graph can be seen on the Figure 19.

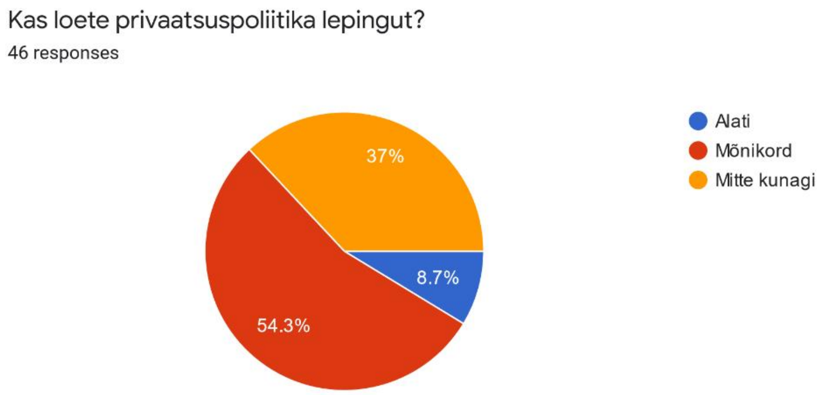


Figure 20 Survey question 13

Do respondents ever read the privacy policy? 8.7% of respondents always read the privacy policy, 54.3% read it sometimes and 37% never read it. The graph can be seen on the Figure 20.

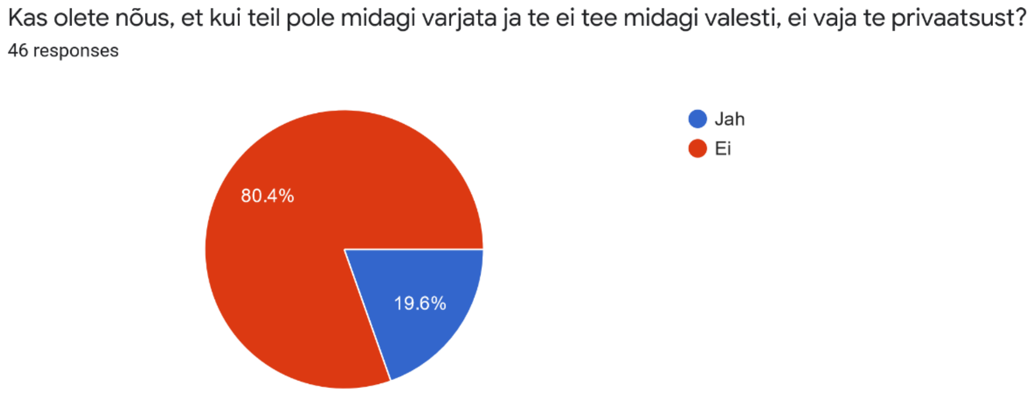
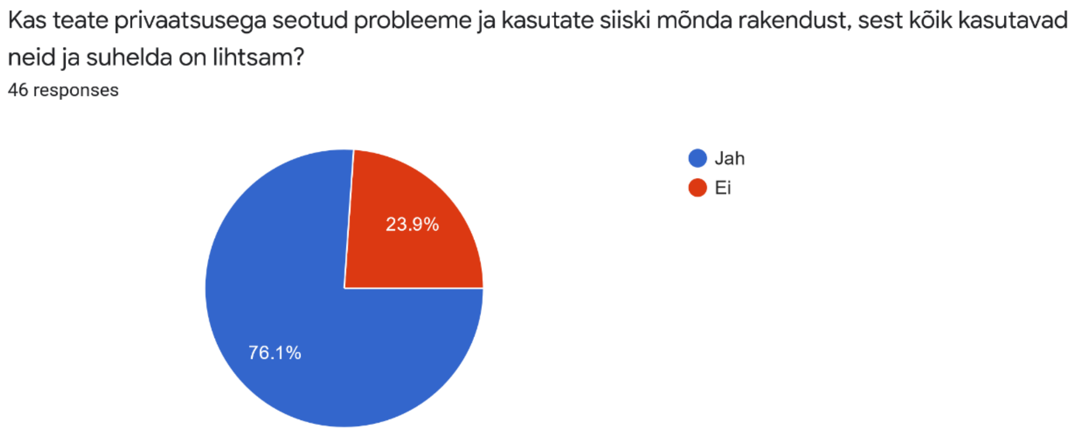


Figure 21 Survey question 14

Do respondents think, that if they have nothing to hide and they do nothing wrong – they do not need privacy? 80.4% do not agree with that statement and 19.6% agree. The graph can be seen on the Figure 21.

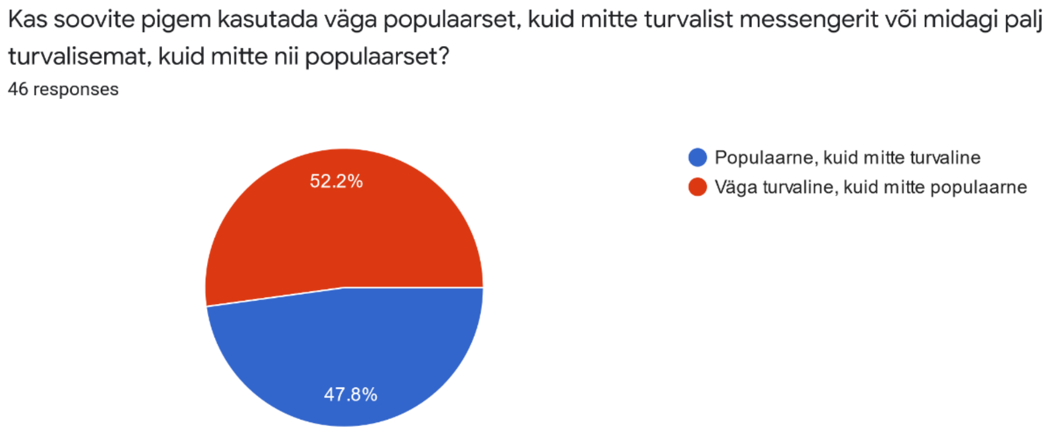


Kas teate privaatsusega seotud probleeme ja kasutate siiski mõnda rakendust, sest kõik kasutavad neid ja suhelda on lihtsam?

46 responses

Figure 22 Survey question 15

Do respondents know about some vulnerabilities but still use non-secure application because everyone use it and it is easier to communicate? 76.1% of respondents agree, 23.9% disagree. The graph can be seen on the Figure 22.



Kas soovite pigem kasutada väga populaarset, kuid mitte turvalist messengerit või midagi palju turvalisemat, kuid mitte nii populaarset?

46 responses

Figure 23 Survey question 16

Do respondents want to use very popular but not secure messenger or something much more secure but not so popular? 52.2% want to use not so popular but more secure messenger. 47.8% want to use popular but not secure. The graph can be seen on the Figure 23.

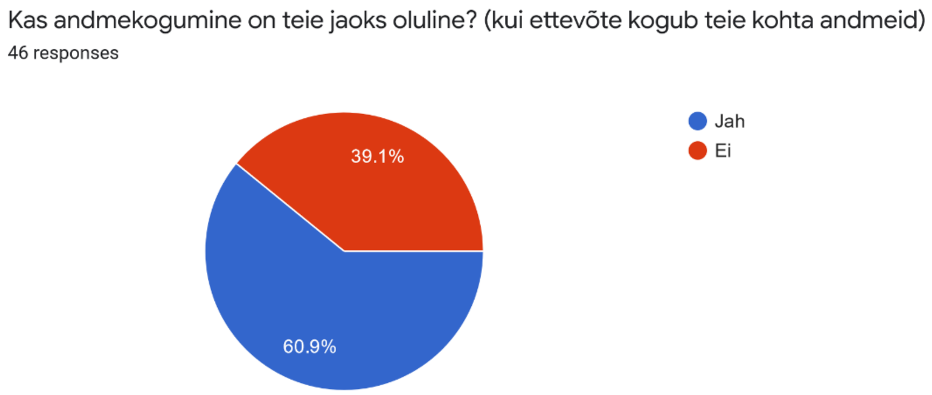


Figure 24 Survey question 17

Is data collection important for respondents? 60.9% are concerned about their data being collected and 39.1% do not consider it as an issue. The graph can be seen on the Figure 24.

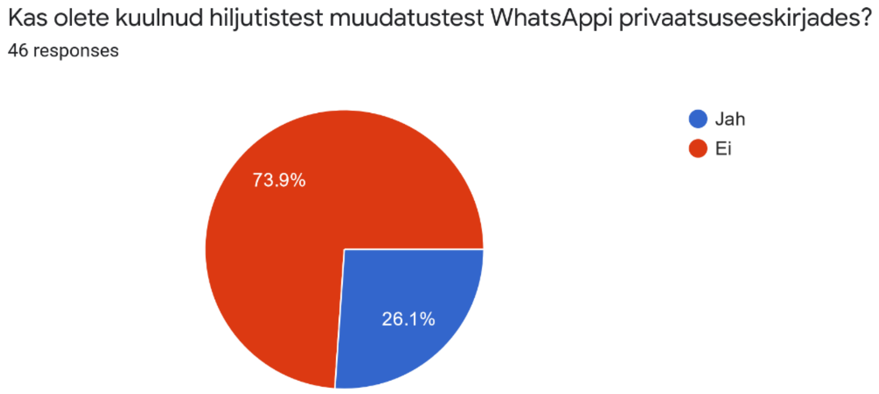


Figure 25 Survey question 18

Did respondents hear about the recent changes in WhatsApp privacy policy? 73.9% did not hear, 26.1% heard about this. The graph can be seen on the Figure 25.

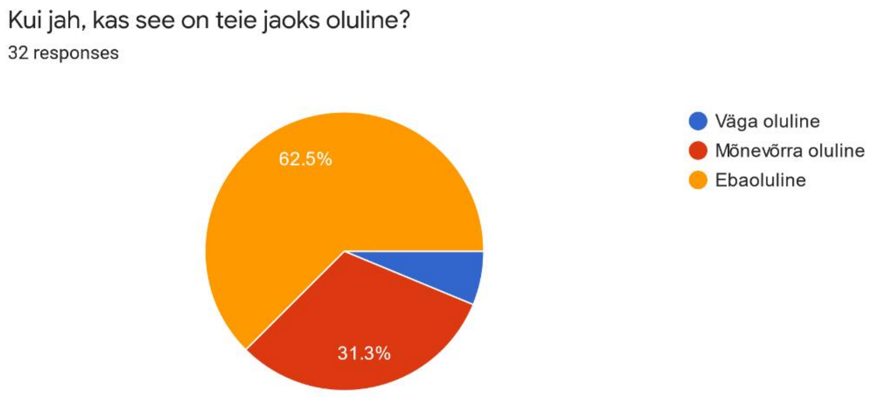


Figure 26 Survey question 19

Of those who heard about it, how important it is to the respondents? 62.5% do not care, 31.3% think that it is important is some way and 6.3% think that this is very important. The graph can be seen on the Figure 26.

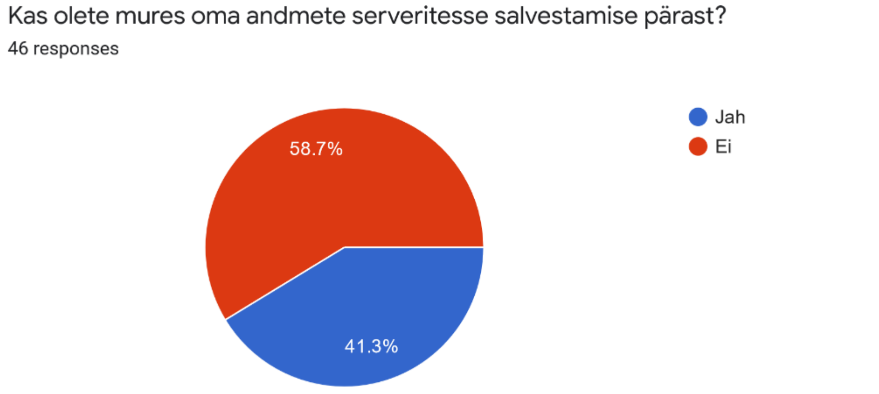


Figure 27 Survey question 20

Are respondents concerned about their data being stored on the servers? 58.7% are not concerned, 41.3% are concerned. The graph can be seen on the Figure 27.

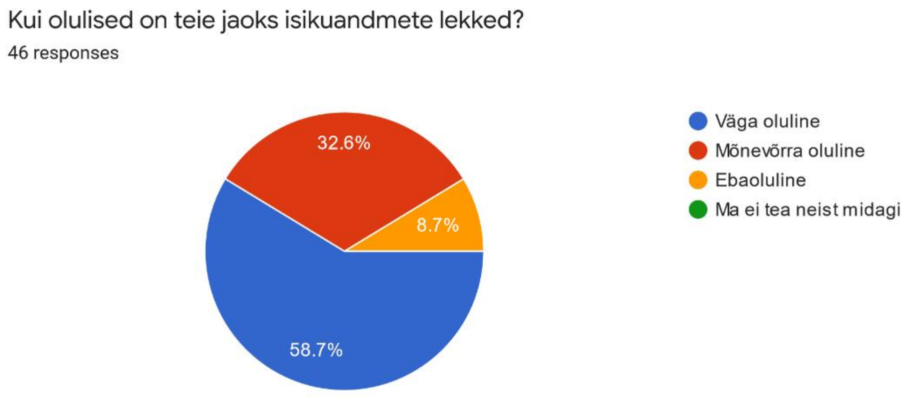


Figure 28 Survey question 21

How important are data leaks for respondents? 58.7% think that this is important, 32.6% think that this is somewhat important and 8.7% do not consider it as an issue. The graph can be seen on the Figure 28.

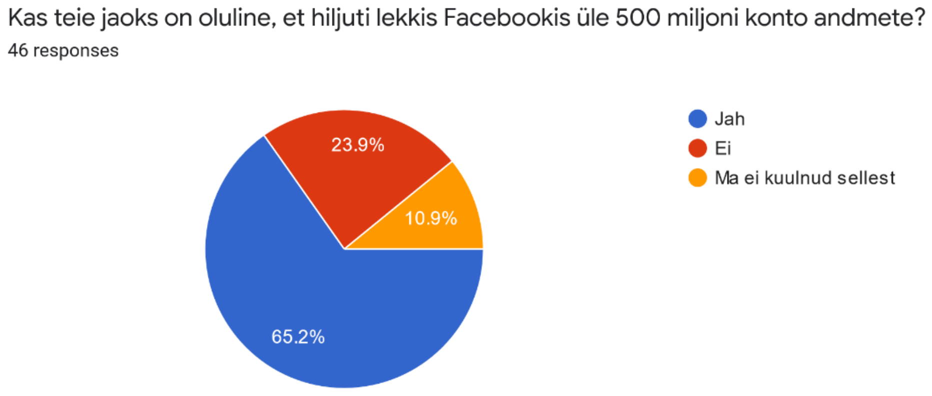


Figure 29 Survey question 22

Is it important for you that recently Facebook had over 500 million accounts data leak? 65.2% consider it important, 23.9% think that this is not important and 10.9% did not hear about that at all. The graph can be seen on the Figure 29.

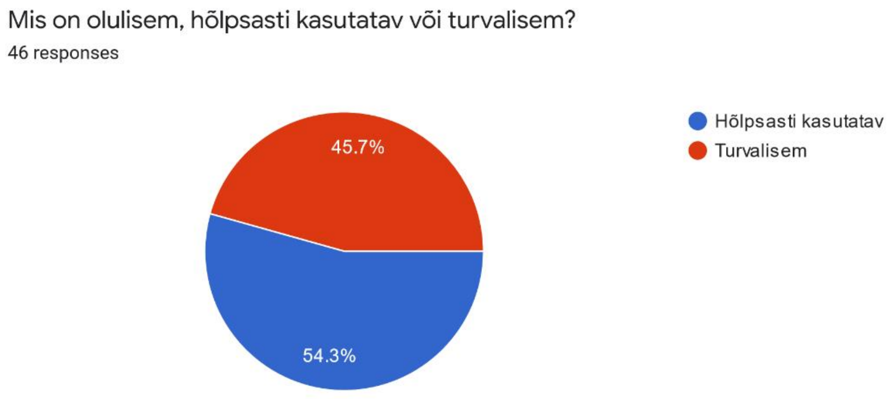


Figure 30 Survey question 23

What is more important, easy to use or more secure? 54.3% think that easy to use is more important and 45.7% want messenger to be more secure instead of easy to use. The graph can be seen on the Figure 30.

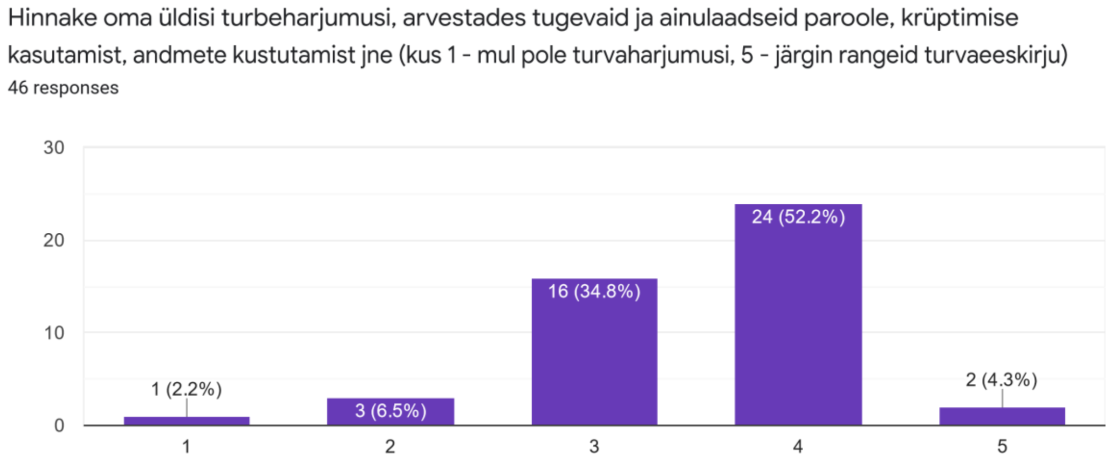


Figure 31 Survey question 24

Rate your overall security habits considering strong and unique passwords, usage of encryption, deletion of data etc. (Where 1 - I do not have security habits, 5 - I follow strict security rules). One of the respondents has no security habits, 6.5% have rated their privacy at 2, 34.8% have rated their security habits at 3, 52,2% at 4 and only 2 respondents have strict security rules. The graph can be seen on the Figure 31.

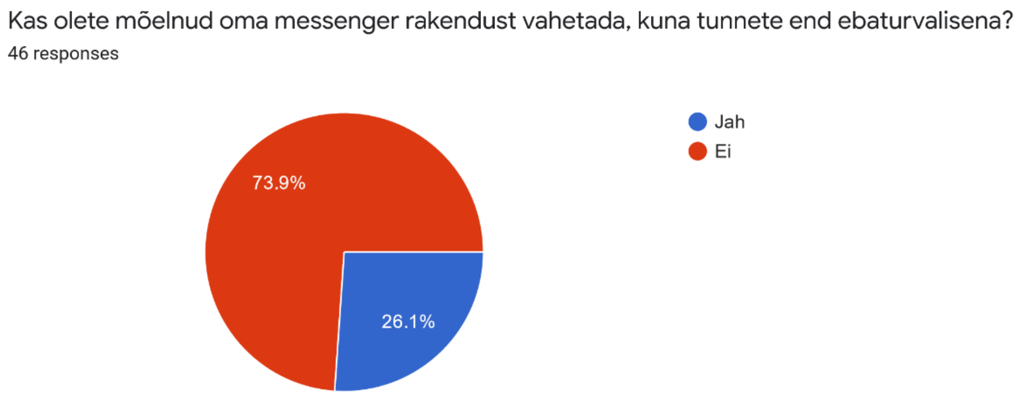


Figure 32 Survey question 25

Do respondents think about changing their messenger app? 73.9% do not want to change, 26.1% want to change. The graph can be seen on the Figure 32.

4.2.2 Analysis of the Survey

From all the answers, it is possible to make a list of the facts that were learned about the respondents:

- Most of the respondents use Facebook Messenger and WhatsApp
- Most respondents value groups, channels, calls, video calls, voice and video messages, cloud synchronization, and ability to archive chats. Most of these functions are present in modern messengers.
- Most respondents value password protection, 2-step verification, cryptography, device linking and unlinking ability, limited data collection, privacy by default.
- Only half of the respondents value end-to-end encryption.
- Most respondents rarely read privacy policy or never read it.
- Most respondents are concerned about the data collection.
- Most respondents do not think that changes in privacy policy in WhatsApp is important to them.
- Most respondents are not concerned about their data being stored on servers

- Half of the respondents think that data leaks are important.
- Most respondents are concerned about Facebook data leaks
- Most of the respondents believe that privacy is important even when they have nothing to hide
- Most respondents use some applications only because others use them.
- Half of the respondents value privacy and security over popularity.
- Half of the respondents value easy-to-use over privacy
- Most of the respondents ranked their privacy habits at 4 out of 5
- Most of the respondents do not want to change their messenger application.

Considering all the factors, it is possible to conclude that people need privacy and security, but they are not ready to sacrifice convenience and ease of use for this. If we consider all the instant messengers that were described in this study, then Telegram would be the better option. Telegram has all the functionality that most respondents value, has a lot of communities and groups, cloud synchronization etc. Some respondents value end-to-end encryption, while some do not need it. Telegram has end-to-end encryption as an optional feature, so it is possible to choose. Most respondents are concerned about the data collection, Telegram does not collect data for advertisement purposes and does not need much data for functionality.

Half of the respondents think that data leaks are important, the only leaks related to Telegram were because of vulnerability in phone number search function that had been fixed with a feature of hiding the phone number from everyone. Most respondents use messengers because of popularity, and it is easy to use. As it is found out in the theoretical part, Telegram has over 500 millions of users and increases its popularity. Also, as Telegram states, the main goal of its messenger is to be fast, easy to use and private.

The prime option for even more security would be the Signal, but at the moment few people use it, and its functionality is only developing, so if people switch from such a multifunctional and convenient messenger as Facebook Messenger, it will be much harder for them to adapt.

4.3 Recommendations

As it can be seen, not all messengers are safe and private. However, there are instant messengers that can provide a high level of security, but at the same time be easy to use and convenient. But what makes them different from each other and how can other messengers become just as safe?

As it is seen from the Table 1, secure messengers differ not only in the set of features that increase security, but also in the way the company itself treats user data. The most insecure messengers collect the most user data and use it for marketing purposes or generally store it in an unencrypted form. With this attitude to data, even the best security settings will not be able to secure users.

That is why the most important recommendations for other messengers will be:

- Collect as less data as it is possible and only for the purposes of messenger functionality.
- Provide users with the ability to set up security and privacy features.
- Always have the support of end-to-end encryption, as well as encryption in transit and encrypted data on the servers.
- Do not store personal data on the servers and delete it as soon as it is not needed.

When companies start to truly value the data of users, then it is possible for messengers to become more secure and private. Even if some leaks occur, storing less data can minimize the threat. If a messenger has end-to-end encryption, a large number of security features but it collects an enormous amount of personal data and uses targeted advertisement – it will never be truly secure and private, as it is seen on the example of the most popular messengers.

5 Conclusion

The goal of this thesis was to analyse the most popular messenger applications in the terms of security and privacy, conduct a survey to know the opinion of users on the topic of the most needed IM application features and security concerns to combine the information gained and choose the most fitting but also secure and private messenger.

During the research, all chosen messengers were compared and a table was created to visually demonstrate the difference between IM applications. The features that are present in the table are the most valuable and common features that are present in the modern messengers, as well as suggestions and wishes of the focus group that were gained from the survey itself. The survey was conducted not only for the sake of understanding the needs of respondents but also to understand the attitude toward security and privacy.

In the end, having all the information combined, the most optimal messenger was chosen that corresponds to the needs of respondents and has good security and privacy features to ensure secure and easy to use experience.

Also, recommendations were given on the topic of securing modern messenger application and making them more private.

References

[1] Syed Aftab Hassan Bukhari, “What is Comparative Study by Syed Aftab Hassan Bukhari :: SSRN,” Jan. . https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1962328 (accessed May 08, 2021).

[2] Saul McLeod, “Questionnaire: : Definition, Examples, Design and Types | Simply Psychology,” 2018. https://www.simplypsychology.org/questionnaires.html (accessed May 09, 2021).

[3] International Committee of the Red Cross, “Humanitarian Futures for Messaging Apps: Understanding the Opportunities and Risks for Humanitarian Action,” p. 98, 2017, [Online]. Available: https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

[4] G. W. Larson, “Instant messaging | communication | Britannica.” https://www.britannica.com/topic/instant-messaging (accessed Apr. 21, 2021).

[5] B. Barry, “a Pplications , and R Esearch D Irections,” no. July 2010, pp. 17–25, 2015.

[6] “What is Client-Server? Definition and FAQs | OmniSci.” https://www.omnisci.com/technical-glossary/client-server (accessed Apr. 22, 2021).

[7] “P2P (Peer To Peer) Definition.” https://techterms.com/definition/p2p (accessed Apr. 22, 2021).

[8] “• Most popular messaging apps | Statista.” https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (accessed Apr. 22, 2021).

[9] “About WhatsApp.” https://www.whatsapp.com/about/ (accessed Apr. 22, 2021).

[10] Parmy Olson, “Facebook Closes $19 Billion WhatsApp Deal,” Oct. 06, 2014. https://www.forbes.com/sites/parmyolson/2014/10/06/facebook-closes-19-billion-whatsapp-deal/?sh=7d5f31075c66 (accessed Apr. 22, 2021).

[11] “WhatsApp Help Center - About two-step verification.” https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=en (accessed Apr. 23, 2021).

[12] Samuel Gibbs, “WhatsApp improves message security with two-step verification | WhatsApp | The Guardian,” Feb. 10, 2017. https://www.theguardian.com/technology/2017/feb/10/whatsapp-improves-message-security-with-two-step-verification (accessed Apr. 23, 2021).

[13] “WhatsApp Help Center - About registration and two-step verification.” https://faq.whatsapp.com/general/verification/about-registration-and-two-step-verification (accessed Apr. 23, 2021).

[14] “WhatsApp Help Center - About disappearing messages.” https://faq.whatsapp.com/general/chats/about-disappearing-messages/?lang=en (accessed Apr. 23, 2021).

[15] “Introducing Disappearing Messages on WhatsApp - About Facebook,” Nov. 05, 2020. https://about.fb.com/news/2020/11/introducing-disappearing-messages-on-whatsapp/ (accessed Apr. 23, 2021).

[16] “WhatsApp Help Center - How to use Android fingerprint lock.” https://faq.whatsapp.com/android/security-and-privacy/how-to-use-android-fingerprint-lock/?lang=en (accessed Apr. 23, 2021).

[17] “WhatsApp Help Center - How to use Touch ID or Face ID for WhatsApp.” https://faq.whatsapp.com/iphone/security-and-privacy/how-to-usetouch-id-or-face-id-for-whatsapp/?lang=en (accessed Apr. 23, 2021).

[18] “WhatsApp Help Center - Security Code Change Notification.” https://faq.whatsapp.com/general/security-and-privacy/security-code-change-notification (accessed Apr. 23, 2021).

[19] “WhatsApp Help Center - Suspicious links.” https://faq.whatsapp.com/android/security-and-privacy/suspicious-links (accessed Apr. 23, 2021).

[20] Madelyn Bacon, “What is end-to-end encryption (E2EE)? - Definition from WhatIs.com,” Jul. 2015. https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE (accessed Apr. 23, 2021).

[21] “WhatsApp Help Center - About end-to-end encryption.” https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption (accessed Apr. 23, 2021).

[22] Kaspersky Team, “What is end-to-end encryption and what are its pros and cons | Kaspersky official blog,” Sep. 11, 2020. https://usa.kaspersky.com/blog/what-is-end-to-end-encryption/23288/ (accessed Apr. 23, 2021).

[23] “Advantages and disadvantages of biometrics | Mitek,” Mar. 15, 2021. https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics (accessed Apr. 23, 2021).

[24] “Privacy Policy,” Jul. 20, 2020. https://www.whatsapp.com/legal/privacy-policy (accessed Apr. 23, 2021).

[25] Nate Cardozo, “Making It Easier to Manage Business Conversations on WhatsApp - About Facebook,” Sep. 22, 2020. https://about.fb.com/news/2020/10/privacy-matters-whatsapp-business-conversations/ (accessed Apr. 23, 2021).

[26] Dan Goodin, “WhatsApp gives users an ultimatum: Share data with Facebook or stop using the app | Ars Technica,” Jan. 06, 2021. https://arstechnica.com/tech-policy/2021/01/whatsapp-users-must-share-their-data-with-facebook-or-stop-using-the-app/ (accessed Apr. 23, 2021).

[27] Zak Doffman, “WhatsApp Beaten By Apple’s New iMessage Privacy Update,” Jan. 03, 2021. https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/?sh=5cf6dd443623 (accessed Apr. 23, 2021).

[28] Zak Doffman, “Do You Suddenly Need To Stop Using WhatsApp?,” Jan. 09, 2021. https://www.forbes.com/sites/zakdoffman/2021/01/09/stop-using-whatsapp-after-facebook-apple-imessage-and-signal-privacy-backlash/?sh=4190539b6cf5 (accessed Apr. 23, 2021).

[29] Katie Canales, “WhatsApp’s New Privacy Policy Delayed Until May 15,” Jan. 15, 2021. https://www.businessinsider.com/whatsapp-privacy-policy-delay-three-months-2021-1 (accessed Apr. 23, 2021).

[30] “WhatsApp Help Center - How to change your privacy settings.” https://faq.whatsapp.com/general/security-and-privacy/how-to-change-your-privacy-settings/?lang=en (accessed Apr. 23, 2021).

[31] “WhatsApp Help Center - How to request your account information.” https://faq.whatsapp.com/general/account-and-profile/how-to-request-your-

account-information (accessed Apr. 23, 2021).

[32] Zak Doffman, “WhatsApp Update Warning As New ‘App Killing’ Message Confirmed: Here’s What You Need To Know,” Dec. 17, 2019. https://www.forbes.com/sites/zakdoffman/2019/12/17/whatsapp-update-warning-as-new-app-killing-message-confirmed-heres-what-you-need-to-know/?sh=3c29ce0d5ad1 (accessed Apr. 24, 2021).

[33] Zak Doffman, “WhatsApp Has Exposed Phones To Israeli Spyware -- Update Your Apps Now,” May 14, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/14/whatsapps-cybersecurity-breach-phones-hit-with-israeli-spyware-over-voice-calls/?sh=1f509d455499 (accessed Apr. 24, 2021).

[34] Kate O’Flaherty, “WhatsApp Users Beware: Here’s How Chats Are Available To Anyone Via Google,” Feb. 22, 2020. https://www.forbes.com/sites/kateoflahertyuk/2020/02/22/whatsapp-users-beware-heres-how-chats-are-available-to-anyone-via-google/?sh=7075f1642d30 (accessed Apr. 24, 2021).

[35] “Messenger - Facts.” https://m.facebook.com/messengerfacts (accessed Apr. 24, 2021).

[36] “What is two-factor authentication and how does it work on Facebook? | Facebook Help Centre.” https://www.facebook.com/help/148233965247823 (accessed Apr. 24, 2021).

[37] “How do I get alerts about unrecognised logins to Facebook? | Facebook Help Centre.” https://www.facebook.com/help/162968940433354?helpref=search&sr=1&query=login alerts (accessed Apr. 24, 2021).

[38] “What are message requests? | Facebook Help Centre.” https://www.facebook.com/help/907368596013605?helpref=search&sr=1&query=message request&search_session_id=335446fa0139f470a6b452ad8d416df2 (accessed Apr. 24, 2021).

[39] “Messenger Privacy & Safety.” https://www.messenger.com/privacy (accessed Apr. 24, 2021).

[40] “How do I set my message to disappear in a Messenger secret conversation? | Messenger Help Centre.” https://www.facebook.com/help/1039542879410863 (accessed Apr. 24, 2021).

[41] “Secret Conversations | Messenger Help Centre.” https://www.facebook.com/help/messenger-app/1084673321594605/ (accessed Apr. 24, 2021).

[42] Zak Doffman, “Why You Should Stop Using Facebook Messenger,” Jul. 25, 2020. https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/?sh=1f5e28ce69ad (accessed Apr. 24, 2021).

[43] “(20+) Facebook.” https://www.facebook.com/policy.php (accessed Apr. 24, 2021).

[44] Kalev Leetaru, “It Turns Out We’ve Been Concerned About Facebook’s Privacy Since The Beginning,” Mar. 11, 2019. https://www.forbes.com/sites/kalevleetaru/2019/03/11/it-turns-out-weve-been-concerned-about-facebooks-privacy-since-the-beginning/?sh=2426fe8a19aa (accessed Apr. 24, 2021).

[45] “Facebook - Full Privacy Report,” Dec. 01, 2020. https://privacy.commonsense.org/privacy-report/Facebook (accessed Apr. 24,

2021).

[46] Jonathan Vanian, “Facebook CEO Mark Zuckerberg Gets Reputation Hit After Data Blunders | Fortune,” Nov. 08, 2018. https://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation/ (accessed Apr. 25, 2021).

[47] Emma Woollacott, “Facebook Fined $645,150 Over Cambridge Analytica Scandal - And Is Told It’s Getting Off Lightly,” Oct. 25, 2018. https://www.forbes.com/sites/emmawoollacott/2018/10/25/facebook-fined-645150-over-cambridge-analytica-scandal-and-is-told-its-getting-off-lightly/?sh=6f34406e2c34 (accessed Apr. 25, 2021).

[48] Kate O’Flaherty, “Facebook Data Breach -- What To Do Next,” Sep. 29, 2018. https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/?sh=6dce71422de3 (accessed Apr. 25, 2021).

[49] Kate O’Flaherty, “Facebook Just Gave 1.3 Billion Messenger Users A Reason To Delete Their Accounts,” Aug. 14, 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/08/14/did-facebook-just-give-13-billion-users-a-reason-to-delete-their-account/?sh=e6e6c2b1662a (accessed Apr. 25, 2021).

[50] “Alon Gal (Under the Breach) on Twitter: ‘All 533,000,000 Facebook records were just leaked for free. This means that if you have a Facebook account, it is extremely likely the phone number used for the account was leaked. I have yet to see Facebook acknowledging this absolute negligence of your data. https://t.co/nM0Fu4GDY8’ / Twitter.” https://twitter.com/UnderTheBreach/status/1378314424239460352 (accessed Apr. 25, 2021).

[51] Aaron Holmes, “Stolen Data of 533 Million Facebook Users Leaked Online,” Apr. 03, 2021. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (accessed Apr. 25, 2021).

[52] “Telegram FAQ.” https://telegram.org/faq#q-how-are-secret-chats-different (accessed Apr. 25, 2021).

[53] “MTProto Mobile Protocol.” https://core.telegram.org/mtproto (accessed Apr. 25, 2021).

[54] “End-to-End Encryption, Secret Chats.” https://core.telegram.org/api/end-to-end (accessed Apr. 25, 2021).

[55] “Photo Editor and Passcode Lock.” https://telegram.org/blog/photo-editor-and-passcodes (accessed Apr. 25, 2021).

[56] “Telegram Privacy Policy.” https://telegram.org/privacy#8-who-your-personal-data-may-be-shared-with (accessed Apr. 25, 2021).

[57] “Telegram FAQ.” https://telegram.org/faq (accessed Apr. 26, 2021).

[58] Zak Doffman, “WhatsApp And Telegram Flaw Exposes Personal Media To Hackers, Check Settings Now,” Jul. 16, 2019. https://www.forbes.com/sites/zakdoffman/2019/07/16/whatsapptelegram-issue-has-put-a-billion-users-at-risk-check-your-settings-now/?sh=300aea365ab8 (accessed Apr. 25, 2021).

[59] Zak Doffman, “Telegram Bug ‘Exploited’ By Chinese Agencies, Hong Kong Activists Claim,” Aug. 25, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/25/chinese-agencies-crack-telegram-a-timely-warning-for-end-to-end-encryption/?sh=2e1fce516342 (accessed Apr. 25, 2021).

[60] Helen Partz, “Millions of Telegram Users’ Data Exposed on Darknet,” Jun. 24, 2020. https://cointelegraph.com/news/millions-of-telegram-userss-data-exposed-

on-darknet (accessed Apr. 25, 2021).

[61] “Features | Viber.” https://www.viber.com/en/features/ (accessed Apr. 26, 2021).

[62] “Viber messaging app bought by Japan’s Rakuten - BBC News,” Feb. 14, 2014. https://www.bbc.com/news/business-26186031 (accessed Apr. 26, 2021).

[63] “• Viber: number of registered users 2020 | Statista,” 2020. https://www.statista.com/statistics/316414/viber-messenger-registered-users/ (accessed Apr. 26, 2021).

[64] “Security and Privacy - Viber Support Knowledge Base.” https://help.viber.com/en/security-and-privacy (accessed Apr. 26, 2021).

[65] “Viber Encryption Overview.”

[66] “Viber Privacy Policy | Viber,” Nov. 2019. https://www.viber.com/en/terms/viber-privacy-policy/ (accessed Apr. 26, 2021).

[67] “Viber Ads, Cookies & Tracking Technologies Policy | Viber,” 2021. https://www.viber.com/en/terms/cookies-and-tracking/ (accessed Apr. 26, 2021).

[68] NepaliTelecom, “People facing Viber Hack attempts after the recent data leaks - NepaliTelecom,” Apr. 16, 2020. https://www.nepalitelecom.com/2020/04/people-facing-viber-hack-attempts-data-leaks.html (accessed Apr. 26, 2021).

[69] Zak Doffman, “Signal Vs Telegram—3 Things You Need To Know Before You Quit WhatsApp,” Jan. 14, 2021. https://www.forbes.com/sites/zakdoffman/2021/01/14/3-things-to-know-before-quitting-whatsapp-for-signal-or-telegram-or-apple-imessage-after-backlash/?sh=4e1b846164f6 (accessed Apr. 26, 2021).

[70] “Signal (@signalapp) / Twitter.” https://twitter.com/signalapp/status/1349577579091566592/photo/1 (accessed Apr. 26, 2021).

[71] “Signal Messenger Features – Signal Support.” https://support.signal.org/hc/en-us/sections/360001602792-Signal-Messenger-Features?page=1#articles (accessed Apr. 26, 2021).

[72] “Signal >> Documentation.” https://signal.org/docs/ (accessed Apr. 27, 2021).

[73] “Screen Security – Signal Support.” https://support.signal.org/hc/en-us/articles/360043469312-Screen-Security (accessed Apr. 27, 2021).

[74] “Incognito Keyboard – Signal Support.” https://support.signal.org/hc/en-us/articles/360055276112-Incognito-Keyboard (accessed Apr. 27, 2021).

[75] “Signal >> Terms of Service & Privacy Policy.” https://signal.org/legal/#privacy-policy (accessed Apr. 27, 2021).

[76] “Signal Messenger Features – Signal Support.” https://support.signal.org/hc/en-us/sections/360001602792-Signal-Messenger-Features (accessed Apr. 27, 2021).

[77] Davey Winder, “Signal Messenger Eavesdropping Exploit Confirmed—What You Need To Know,” Oct. 05, 2019. https://www.forbes.com/sites/daveywinder/2019/10/05/signal-messenger-eavesdropping-exploit-confirmedwhat-you-need-to-know/?sh=617682e37dc1 (accessed Apr. 27, 2021).

[78] “About Discord | Our Mission and Values.” https://discord.com/company (accessed Apr. 27, 2021).

[79] “Setting Up Your Account for Privacy & Safety | Discord.” https://discord.com/safety/360043857751-Four-steps-to-a-super-safe-account#1.-Secure-your-account (accessed Apr. 27, 2021).

[80] “Discord | Privacy & security guide | Mozilla Foundation.” https://foundation.mozilla.org/en/privacynotincluded/discord/ (accessed Apr. 27, 2021).

[81] “Privacy Policy | Discord,” Jun. 23, 2020. https://discord.com/privacy (accessed Apr. 27, 2021).

[82] “Your Content Clause Explained – Discord,” 2020. https://support.discord.com/hc/en-us/articles/360018659011-Your-Content-Clause-Explained (accessed Apr. 27, 2021).

[83] “Data Privacy Controls – Discord,” 2020. https://support.discord.com/hc/en-us/articles/360004109911-Data-Privacy-Controls (accessed Apr. 27, 2021).

[84] Lee Mathews, “Gamers Beware: Stealthy Malware Steals Your Discord Password And Attacks Your Friends,” May 25, 2020. https://www.forbes.com/sites/leemathews/2020/05/25/warning-malware-steal-discord-passwords/?sh=3288b2254572 (accessed Apr. 27, 2021).

[85] Andy Greenberg, “Hackers Are Exploiting Discord and Slack Links to Serve Up Malware | WIRED,” Apr. 07, 2021. https://www.wired.com/story/malware-discord-slack-links/ (accessed Apr. 27, 2021).

[86] Jay Peters, “Discord bans the r/WallStreetBets server, but new ones have sprung to life - The Verge,” Jan. 27, 2021. https://www.theverge.com/2021/1/27/22253251/discord-bans-the-r-wallstreetbets-server (accessed Apr. 28, 2021).

[87] Hannah Boland, “Hedge fund-backed Discord accused of censorship after it suspends WallStreetBets,” Jan. 28, 2021. https://www.telegraph.co.uk/technology/2021/01/28/discord-accused-censorship-suspends-wallstreetbets/ (accessed Apr. 28, 2021).

[88] “Snapchat: What is Snapchat?” https://edu.gcfglobal.org/en/snapchat/what-is-snapchat/1/ (accessed Apr. 28, 2021).

[89] Chad Recchia, “Generational Gap: How To Reach Millennials And Gen Zers On Snapchat,” Jul. 12, 2018. https://www.forbes.com/sites/forbesagencycouncil/2018/07/12/generational-gap-how-to-reach-millennials-and-gen-zers-on-snapchat/?sh=38fffea621d1 (accessed Apr. 28, 2021).

[90] “Create a Snap.” https://support.snapchat.com/en-US/article/capture-a-snap (accessed Apr. 28, 2021).

[91] “Set Up Two-Factor Authentication.” https://support.snapchat.com/en-US/article/enable-login-verification (accessed Apr. 28, 2021).

[92] Saima Salim, “Finally: Snapchat comes up with end-to-end encryption to secure users conversations and data / Digital Information World,” Jan. 11, 2019. https://www.digitalinformationworld.com/2019/01/snapchat-end-to-end-encryption-users-media-messages.html (accessed Apr. 28, 2021).

[93] “Privacy Policy - Snap Inc.,” Mar. 24, 2021. https://snap.com/en-US/privacy/privacy-policy (accessed Apr. 28, 2021).

[94] “Advertising & Interest Preferences.” https://support.snapchat.com/en-US/article/advertising-preferences (accessed Apr. 28, 2021).

[95] “Privacy Settings.” https://support.snapchat.com/en-US/article/privacy-settings2 (accessed Apr. 28, 2021).

[96] Lindsey O’Donnell, “Snapchat Privacy Blunder Piques Concerns About Insider Threats | Threatpost,” May 24, 2019. https://threatpost.com/snapchat-privacy-blunder-piques-concerns-about-insider-threats/145074/ (accessed Apr. 28, 2021).

[97] ABC NEWS, “Snapchat’s new Snap Map feature raises privacy concerns - ABC News,” Jun. 26, 2017. https://abcnews.go.com/Lifestyle/snapchats-snap-map-feature-raises-privacy-concerns/story?id=48271889 (accessed Apr. 28, 2021).

[98] Arjun Kharpal, “What is WeChat? Explaining China’s largest messaging app by

Tencent," Feb. 04, 2019. https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html (accessed Apr. 28, 2021).

[99] "Tencent - Tencent 腾讯." https://www.tencent.com/en-us/about.html (accessed Apr. 28, 2021).

[100] "What should I do if I'm unable to unblock my WeChat account?" https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&id=170621ueqe3y170621rr7vqa&lang=en&plat=2&Channel=helpcenter (accessed Apr. 28, 2021).

[101] "All you can do with WeChat in 2020," May 16, 2019. https://qpsoftware.net/blog/all-wechat-features-2020 (accessed Apr. 28, 2021).

[102] M. Chen, L. Clayberg, and H. Li, "Security in the Face of Censorship."

[103] "Privacy Policy." https://www.wechat.com/mobile/en/privacy_policy.html (accessed Apr. 28, 2021).

[104] Anna Rasmussen, "Is WeChat safe to use? | NordVPN," Aug. 28, 2020. https://nordvpn.com/blog/is-wechat-safe/ (accessed Apr. 28, 2021).

[105] "Over 300 million Chinese private messages were left exposed online - The Verge," Feb. 04, 2019. https://www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police (accessed Apr. 28, 2021).

[106] Nikhil Sonnad, "How WeChat censors politically sensitive messages, as revealed by Citizens Lab research — Quartz," Apr. 18, 2017. https://qz.com/960948/what-happens-when-you-try-to-send-politically-sensitive-messages-on-wechat/ (accessed Apr. 28, 2021).

[107] "Tencent Executive Held by China Over Links to Corruption Case - WSJ," Feb. 10, 2021. https://www.wsj.com/articles/tencent-executive-held-by-china-over-links-to-corruption-case-11613009016?mod=hp_lead_pos3 (accessed Apr. 28, 2021).

[108] "Jabber.org FAQ." https://www.jabber.org/faq.html#jabber (accessed Apr. 28, 2021).

[109] "XMPP | An Overview of XMPP." https://xmpp.org/about/technology-overview.html (accessed Apr. 28, 2021).

[110] "jabber.org service policy." https://www.jabber.org/policy.html#default (accessed Apr. 28, 2021).

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Erik-Filipp Oleinikov

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Comparison of Security and Confidentiality Aspects in Modern Messenger Applications”, supervised by Mohammad Tariq Meeran.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.