Katholieke Universiteit Leuven

Master of Statistics and Data Science

Privacy and Big Data

Privacy Impact Assessment: WhatsApp

Author:
Anh Phuong Dinh, r0913033
Frunz Gharagyozyan, r0917476
Xiaoyun Sun, r0919042

January 1, 2023

Contents

1 Introduction

WhatsApp (also called WhatsApp Messenger) is the most widely used messaging application, with more than 2 billion active users worldwide. One may imagine what major consequences may occur in case of possible privacy infringements in the application with such an enormous user base, actively sharing intimate moments of their lives through photos and messages.

Ever since its acquisition by then Facebook in 2014, there has been growing anxiety regarding how WhatsApp may modify its data collection, handling, and sharing approaches to adapt to its parent company's ad-based business model. This concern proved legitimate as Facebook announced a few years later that it had the plan to integrate the messaging systems of Facebook, Instagram, and WhatsApp in the long run [8]. The momentum away from WhatsApp does appear to be building, especially after the global backlash when it upgraded the privacy policy in 2021. In competition with other non-profit, open-source messaging platforms like Signal, it is no wonder that WhatsApp's mission to gain back the trust of the user base remains challenging.

In this report, we will present the techniques WhatsApp uses to ensure secure communication, identify potential threats to the system and advise new strategies to increase the privacy protection level in the application. The methodological framework in use is LINDDUN, which provides a systematic approach to modeling privacy threats [6].

The organization of the report is as follows.

- Section 2 gives a thorough description of the WhatsApp system, including its functionality, stakeholders, data collection.
- Section 3 examines WhatsApp's design and implementation and suggests a Data Flow Diagram (DFD) based on LINDDUN approach.
- In Section 4, we present a table that maps each element in DFD to LINDDUN categories of privacy threats and give an interpretation of risks in Section 5.
- In Section 6, we propose strategies to mitigate those privacy issues.

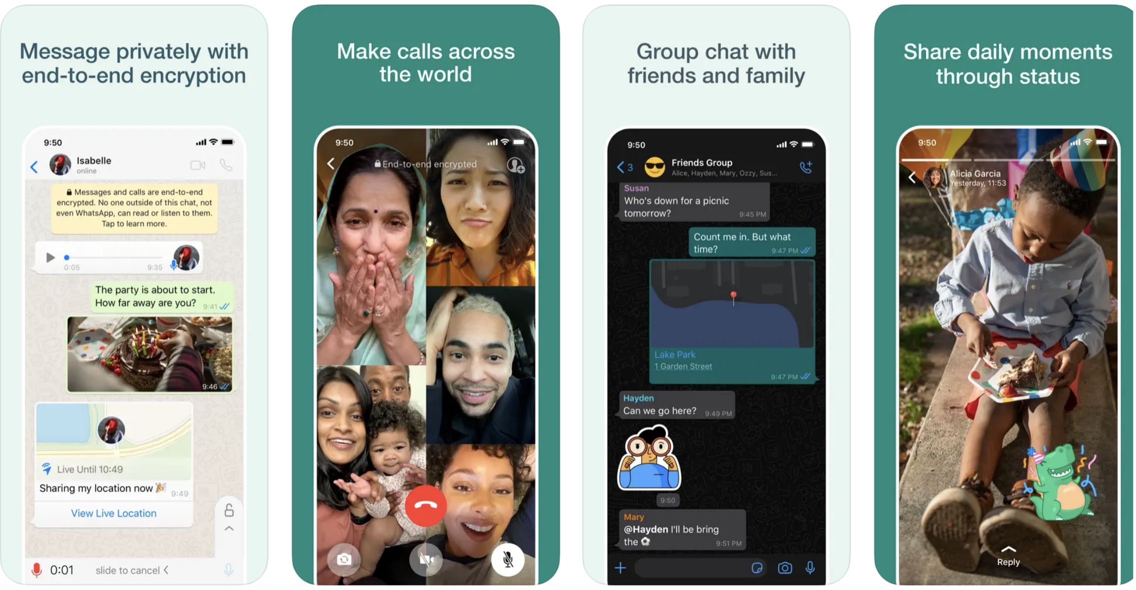
2 Product description

2.1 Functionality

The main function of WhatsApp is secure messaging, video, and voice calling. Since 2014, WhatsApp has partnered with Open Whisper Systems to integrate the Signal Protocol into their product, moving towards full end-to-end encryption (E2EE) for all users by default [19]. Neither intermediaries (WhatsApp server, database) nor any bad actors would be able to read the message you send as only the recipient would have the key to decrypt it. WhatsApp allows users to participate in group chats, send and receive documents, video and audio files, and share their location. Besides, it is possible to send disappearing messages, look for a specific message in the chat, prioritize them with stars, forward them to other people, and more.

The application provides additional information about every message indicating whether it was delivered, read, or played in the case of media files. To improve the quality of user experience in the application, WhatsApp chats may be customized, varying in the interface design to satisfy particular users' needs and preferences.

WhatsApp is also available on the web and desktop and can be easily synchronized with the mobile app providing a continuous and reliable messaging process. Although they planned to roll out the multi-device architecture by 2021, the current version still relies on the smartphone as the primary device, making the phone the source of truth for all user data and the only device capable of end-to-end encrypting messages for another user. Therefore, the mobile app will be the primary focus of this report.



Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

The party is about to start. How far away are you?

Sharing my location now 🎉

Susan
Who's down for a picnic tomorrow?

Count me in. But what time?

Lake Park
1 Garden Street

Hayden
Can we go here?

Mary
@Hayden I'll be bring the ✿

Figure 1: WhatsApp mobile app's user interface

2.2 Stakeholder identification

The stakeholders involved in WhatsApp include any entity related to the app's operation, that is naturally exposed to the data or is impacted by the data collected. As the service provider, WhatsApp is responsible for collecting, processing, and disseminating all user data and thus is considered a data controller.

- The prime stakeholders of WhatsApp are the end users - individuals who use the application to communicate and thus might share a number of personal information in the process. Because information about one's contacts (including those in the address book, those who contact the user but are not in his address book, and those who are blocked and blocked the user) is available on WhatsApp, these people are also considered user stakeholders.

Several third-party stakeholders include individuals, third-party services, and service providers.

- Third-party individuals are those who have interaction with the user, are in the same group, or have the user's phone number. It is obvious as the receiver of messages and media can view, store or reshare this content on and off WhatsApp. Similarly, these users can see one's account information or can add one to groups where their personal information is visible to others. Whoever has the user's phone number is also aware of their "last seen" or receipt status, although this can be changed in the privacy settings.
- When users or those who interact with users use third-party services, the providers of those services may receive the information about the user they or others share. More importantly, being a part of Meta Platform Inc., WhatsApp actively shares the data collected with other Meta Companies worldwide as these companies provide data hosting, infrastructure services, technical engineering support, and perform business analytics.
- Lastly, the regulators, law enforcement, other government agencies, industry partners/peers such as other online platforms and technology companies, and WhatsApp's advisors such as external lawyers are stakeholders as well. It is the responsibility of law enforcement and public bodies to ensure that the appropriate laws are followed.

2.3 Data collection

Information Provided by users [12]:

- Account Information: The user's mobile phone number and profile name are used to create a WhatsApp account. Additional optional information is collected, such as profile pictures and "about" information.

- User Content: Messages, Media within messages, and calls.
  Typically messages are stored on users' devices and not on WhatsApp servers, but an encrypted form is stored while the contents are being delivered. Once the contents are delivered, they are deleted from WhatsApp servers. WhatsApp stores the encrypted messages on its server for 30 days while trying to deliver them. If the messages were not to be delivered in 30 days, they were deleted from the server. The contents of the messages can not be read by WhatsApp as they are encrypted. Status: end-to-end encrypted.

- Precise Location Information: Precise location information is shared when users use location-related features. Precise location information is encrypted as well. Profile pictures, users' "about" information, names, and descriptions of users' groups are not encrypted.

- Connections: The Contact Upload feature regularly shares the phone numbers of users' address books with WhatsApp. Users who are blocked by one user or who have blocked the user, will also be identified through phone numbers.

- Group Information: Information regarding groups user created or updated will be collected. This information includes the status of creating, joining, and being added, as well as the name, group profile picture, and description.

- Customer Support Information and other communications:

- Account Access Information Code sent via SMS when users sign up or log in.

Automatically collected information

- Usage information: information about user activity, user interaction with other users or businesses, and the time, frequency, and duration of activities.

- Logs and troubleshooting information: service-related diagnostic and performance information, which includes log files, timestamps, diagnostic or crash data, website performance logs, and error reports.

- Device and connection information: hardware model, operating system information, battery level, signal strength, app version, browser information, mobile network, connection information regarding WiFi or cellular data, mobile operator or ISP, language and timezone, IP address, device operation information and identifiers (including identifiers unique to Meta Company Products)

- General location information

- Cookies

- User choice: in-app settings, privacy settings, and records about the acceptance of Terms.

- Authentication information: public encryption keys

3 Architecture

3.1 Data flow diagram

Based on LINDDUN methodological framework [6], we analyze WhatsApp's system using the Data Flow Diagram (DFD) as the preliminary step to capture the most relevant system knowledge for privacy analysis. DFD consists of external entities (i.e., users or third-party services external to the system), processes (i.e., an activity that changes or transforms data flows), data stores (i.e., containers of information), and data flows (i.e., movement of data between external entities, processes and data stores). Thus, DFD provides a visual representation that maps out how information is generated, stored, processed, and disseminated through the system.

As indicated by the diagram, the entities are

- User
- Individuals on WhatsApp
  (i.e., the individuals in contact with the user, the individuals who receive the User's Content or are in the same group chat with the user
- Third-party service providers
  (e.g., Meta Companies, data backup services such as iCloud or Google Drive).

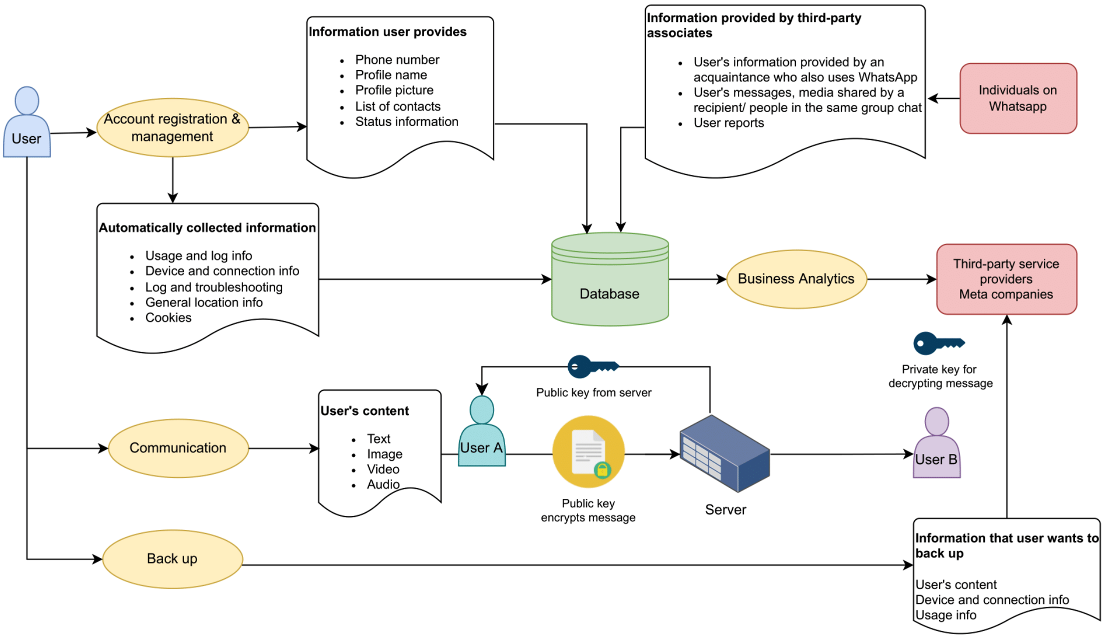

User
Account registration & management
Information user provides
Phone number
Profile name
Profile picture
List of contacts
Status information
Information provided by third-party associates
User's information provided by an acquaintance who also uses WhatsApp
User's messages, media shared by a recipient/ people in the same group chat
User reports
Individuals on Whatsapp
Automatically collected information
Usage and log info
Device and connection info
Log and troubleshooting
General location info
Cookies
Database
Business Analytics
Third-party service providers
Meta companies
Private key for decrypting message
Public key from server
User's content
Text
Image
Video
Audio
Communication
User A
Public key encrypts message
Server
User B
Back up
Information that user wants to back up
User's content
Device and connection info
Usage info

Figure 2: Data Flow Diagram for WhatsApp's application

When a user registers and manages their account, it is mandatory to provide a phone number and profile name of choice to use the Service. Online identifiers (usage and log information, IP address, mobile operator, language and time zone...) are automatically collected and stored in the WhatsApp database, along with information about the user provided by third-party individuals and businesses on WhatsApp. This information might be shared with Meta Companies and other third-party service providers to perform business analytics.

Among the processes, business analytics refers to the disciplines utilizing collected data to gain insights and solve business problems. As stated by WhatsApp, the general goal is to obtain engineering and operation support, assist in customer service, and help WhatsApp understand how people use their services and market them, among other things.

3.2 Design and Implementation

WhatsApp's system architect consists of two parts: the front end and the back end. The front end part is the mobile or web app that a user interacts with. WhatsApp supports nearly all platforms, including iOS, Android, Windows and OSX desktop, web app, and Windows Phone app. Besides the User Interface, the application also comes with a SQLite database that stores chat locally in the user's devices.[2] The backend consists of WhatsApp cloud servers that serve as the messenger between users and store the encrypted messages temporarily while the message is being delivered. Once the user on the receiving end of the message opens the application, the queued message will be routed from the cloud server and delivered to the recipient. Once the delivery is confirmed, the encrypted message will be deleted from WhatsApp's database.

WhatsApp uses end-to-end encryption, which means that only the original sender and the desired recipient should be able to read the message in plain text. WhatsApp chose Signal Encryption Protocol[1] as its encryption method, and the communication between the server and its clients is through a highly modified version of XMPP.

4 Privacy Analysis

4.1 LINDDUN privacy analysis

The abstract table in Figure 2 indicates the determination of privacy threats based on the elements of the Data Flow Diagram. Each DFD element is potentially susceptible to specific privacy threats belonging to 7 high-level categories following the LINDDUN threat modeling approach [6]. The explanation with examples is given below.

Linkability: is when all events or records belonging to the same data subject can be linked together. Although linkability is not a privacy issue in and of itself, there is a direct relationship between linkability and identification and inference, which could lead to profound societal consequences.

Identification: The ability to correctly assign an event or record to an identifiable or known individual with a high probability. Several WhatsApp user's basic features, such as profile name, profile image, and phone number, make it possible to identify the user and his presence on other social networking platforms.

Non-repudiation: The person cannot deny his association with a piece of information and, thus, can be held accountable for a claim. For instance, a WhatsApp user cannot deny his association with a group and interactions/transactions with a WhatsApp business account.

Detectability: An adversary can learn specific information about a subject by detecting the existence of an item of interest without knowing the exact information. For example, by knowing that a person joins multiple groups of KUL students on WhatsApp, one can assume that the person is most likely studying in Leuven now without having access to their academic record. It is safe to deduce that person might be interested in renting a flat in Leuven or in other services targetting students.

Disclosure of information: This involves exposing information to individuals who are not supposed to have access to it. A WhatsApp user or a user of any messaging app is prone to the risk of having their texts, media and calls recorded and leaked to outsiders without their knowledge or consent.

Unawareness: Users are usually unaware of the information they supply to the system and the impact of sharing data. End-to-end encryption protects WhatsApp conversations, but users might need to realize that metadata (phone model, IP address, transactional data, usage and log information, cookies) might be collected, analyzed, and shared with third parties for profiling purposes.

Non-compliance: WhatsApp must inform the data subject about the system's privacy policy and allow the data subject to specify consent in compliance with legislation before users access the system.

Table 1: Mapping LINDDUN components to DFD elements types .

Types	Threat target	L	I	N	D	D	U	N
Entity	User	1	2	x	3	4	5	x
	Individuals on WhatsApp	6	7	x	x	x	8	9
	Third-party service providers	x	x	x	x	x	x	10
Data store	Database	x	x	x	x	x	x	11
Data flow	Information user provides → Database	12	13	x	x	x	x	x
	Automatically collected information → Database	14	15	x	16	x	17	18
	Information provided by third-party associates → Database	19	20	x	x	x	21	x
	Information user wants to back up → Database	x	x	x	x	22	23	24
	User's content → Individuals on WhatsApp	x	x	x	x	x	x	x
	Database → Third-party service providers/ Meta companies	x	x	x	x	25	26	27
Process	Business Analytics	28	x	x	x	x	29	30

Note: x signs used in the table indicate no threats.

5 Risks

5.1 Technical risks

1. Reliance on the security of third-party services (Threat 22, 23, 24)

The end-to-end encryption of the messages means that only one user who is the original receiver may decode the content of the message. In reality, it is not always the case as WhatsApp offers to back up the information and store it in Google Drive or iCloud. As the encryption of these backup files is not mandatory, WhatsApp relies on the security of those storage providers. At the end of 2021, WhatsApp claimed to offer end-to-end backup encryption [24]. However, this function has not been rolled out to every devices and there is no update about its implementation for the time being.

2. Metadata of the messages (Threat 4, 5, 25, 26, 27, 14, 15)

In their Privacy Policy, WhatsApp states that *"end-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp."* [11] The end-to-end encrypted messaging process makes it extremely difficult to get the content of the message even in case of possible success in hacking the system. However, this does not necessarily mean that any adversary or even WhatsApp can not retrieve information about the size of the message or file and the sending date. Users' messaging frequency and additional details of the messages or files can be used to model the user behavior even when the user does not grant such permission.

3. Threats of re-identification (Threat 1, 2, 6, 7, 12, 13)

WhatsApp employs an encryption technique known as "lossy hashing" which converts a real phone number into a shorter code that is then made available to other parties. Even though WhatsApp claimed this technique anonymized the data and so no longer comprised "personal data," the EDPB (European Data Protection Board) discovered that WhatsApp had a method of decrypting and recovering the data; thus, this should be treated as a pseudonymization method instead. By definition, the data is considered anonymous if it is processed so that it can no longer be used to directly or indirectly identify a natural person using *"all the means reasonably likely to be used"* by either the controller or a third party. However, considering the tools and data accessible to WhatsApp, the potential to identify data subjects is too high to consider the dataset anonymous [10].

5.2 Legal risks

WhatsApp operates almost globally with few exceptions due to political decisions; therefore, the company should handle varying data protection regulations and protocols across countries and regions. This report will discuss a few legal risks based on the General Data Protection Regulation (GDPR) [13], which governs how the personal data of individuals within the European Union may be transferred and processed. The idea behind GDPR can be summarized in 7 main principles [22] as follows:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

WhatsApp is constantly making effort to adhere to GDPR's requirements, especially after getting one of the largest fines in the history of 225 million euros by Ireland's data watchdog [25]. However, there are still several aspects that should be considered and discussed in this report.

1. Unawareness of data processing and transfer to third-party providers (Threat 1, 28, 29, 10, 30)

The data transfer between WhatsApp and third-party providers such as Meta companies is one of the critical issues that led to WhatsApp receiving a fine [25]. In the Privacy Policy [11], they state *"we work with third-party service providers and other Meta Companies to help us operate, provide, improve, understand, customize, support, and market our services."* Also, they provide a link to another section about this cooperation, where they declare, *"we may use the information we receive from them, and they may use the information we share with them"*. In this statement, WhatsApp does not mention the specific types of data they share and how the data is processed, making it impossible to determine if tasks must be completed. This ambiguity undermines the GDPR's transparency concept, emphasizing the user's access to information [21]. To be specific, it could be seen as a violation of **GDPR (Article 4.11)** [17], which states that *"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

2. Unclear Privacy Policy (Threat 26, 29)

In accordance with **GDPR (Article 12.1)**, all information pertaining to the treatment and processing of the subject's data must be provided *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"* [14]. However, it is evident that the contents of WhatsApp's Privacy Policy are inadequately structured and have several ambiguous statements. The current policy does not explicitly mention the specifics of sharing data with third-party businesses: which companies are involved, what data might be shared with them, and for what purpose are only vaguely mentioned. WhatsApp only stated that the data is subject to a *"separate, stand-alone terms of services and privacy policy"* when shared with third parties. This ambiguity makes it challenging for users to understand the process and could be seen as violating the transparency concept.

3. Lack of consideration for privacy-by-design (Threat 9, 18)

GDPR (Article 25) communicates the requirements for data privacy by design and data privacy by default [16]. Fundamentally, privacy by design demands the inclusion of appropriate data protection from the initial design stages throughout the complete life cycle of a product. Data privacy by default implies that (a) only necessary personal data is collected, stored, or processed, and (b) personal information is not available to an infinite number of persons. WhatsApp's uploading and storing of the user's address book does not adhere to the "privacy by design" and "privacy by default" concepts. Also, by making the phone number visible to everyone, WhatsApp allows the spread of user's phone number to *"an indefinite number of natural persons"*.

4. Redundant data collection (Threat 3, 16)

Data minimization principle is represented in **GDPR (Article 5.1.c)** [18], which provides that personal data must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*. WhatsApp collects information about hardware model, operating system, battery level, signal strength, app version, browser information, mobile network, connection information (including phone number, mobile operator or ISP), language and time zone, and IP address [11]. Although most of the data gathered by the app can be de-contextualized to serve different purposes than the ones presented to the user, there is no option for the user to allow certain types of data to be collected selectively. WhatsApp does not explain in depth the necessity of this information to make a stable communication process, which is the application's primary usage.

5. Unjustified purpose for data retention (Threat 11)

The right to be forgotten appears in **GDPR (Article 17)** [15]. It states, *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay"* if one of a number of conditions applies. *"Undue delay"* is considered to be about a month. When deleting a WhatsApp account, a user expects his account information, profile picture, participation in a WhatsApp group, and message history backup to be removed. However, it is implied that WhatsApp retains a copy of the data even after the termination of their services, as stated in the FAQ: *“Copies of your information may also remain after the 90 days in the backup storage that we use to recover in the event of a disaster, software error, or other data loss event”.* They also stated, *“We may also keep your information for things like legal issues, terms violations, or harm prevention efforts”* without elaborating and justifying the necessity of such retention. Users also have to explicitly ask for the right to access, port, and erase certain data via email [9].

5.3 Ethical risks

With the growing popularity among WhatsApp users, ethical concerns have started to surface. Besides ethical issues that map to LINDDUN threats, some occur when cybercriminals take advantage of WhatsApp for the purposes such as digital activism, copyright, or spamming, all of which are not part of WhatsApp intended.

1. Risk of surveillance (Threat 1, 2, 3)

While the messages on WhatsApp are protected by end-to-end encryption, the messaging company shares a variety of metadata with Meta companies, including but not limited to *”account registration information (such as your phone number), transaction data, service-related information, information on how you interact with businesses when using our Services, mobile device information, IP address”.* By analyzing general location data, the business the user interacts with, the frequency of his usage, and the groups he joins, WhatsApp can discover a wealth of information about the user. With this information, they can draw an instructive map of the user’s activities and behaviors to enhance ad-targeting profiles.

2. Risk of spreading mobile number (Threat 12, 13, 1, 2, 6, 7, 8, 5)

WhatsApp utilizes the phone number to validate an account. The number serves as the user’s primary means of identification, no matter how it may be changed. A visible phone number is not a problem in one-on-one communications because both parties are willing to reveal it. However, when users engage in group chats, ethical issues might develop. For instance, users can add their contacts to groups, leading to a situation when two or more people are in the same group without explicit agreement. Even if the owner does not intend it, every user in the same group can access every other phone number. Other messaging services might employ aliases or representatives, which contain less personal information. The inability of the user to hide their phone number is a drawback that might be exploited and lead to unintended repercussions for which WhatsApp should be held accountable.

3. Violation of the copyright

The copyright rules should protect the original author’s rights by treating one work as individual property. People might use WhatsApp to send messages containing copyrighted content of an original piece. WhatsApp provides an option to report the copyright issue, intending to stop the violation of rights. In the terms and conditions, users of WhatsApp agree to it is explicitly mentioned that the violation of someone else's intellectual property is considered a crime. The concern is that WhatsApp can take action only when the users report a copyright issue.

4. Spamming

Spamming is a form of messaging to send unrelated, commercial, non-commercial, harmful, or non-prohibited information to a large number of people. Spam messages can contain viruses to affect the user's device and also hurt the user's feelings and emotions with their offensive content. Currently, the default setting of auto-saving media from WhatsApp group presents a risk where users might be exposed to inappropriate images and videos and the user needs to figure out the setting in order to switch this function off.

6 Recommendations

1. Deploy backup encryption by default

WhatsApp should provide end-to-end encryption for backups by default to reduce the risk of data leakage when users choose to backup their contents using cloud storage. WhatsApp has gradually rolled out the option by the end of 2021, but the feature is not enabled by default and to every device.

2. Enhance phone number privacy

The default setting for sharing a user's phone number with others on WhatsApp must be changed. The best course of action would be to allow users to share their phone numbers with their contacts, other group members, and exclusive users rather than making it public by default. With this update, users will regain control over who may access their phone numbers and identify them.

3. Develop data anonymization process

WhatsApp is currently using "lossy hashing" technique to compress and blur data, including non-user phone numbers. Since there was evidence pointing to WhatsApp's capability to restore this data, data anonymization techniques such as k-anonymity and differential privacy techniques should be developed to make the data genuinely irreversible and can no longer be used to directly or indirectly identify a person. After implementing the new techniques, a re-identification risk analysis should be conducted. Finally, the process and result should be audited and confirmed periodically by third parties and regulators to guarantee the result.

4. Re-formalize the contents of Privacy Policy

The contents of WhatsApp's Privacy Policy should be reviewed and re-written in a clear, transparent, and readable manner to meet the directive of **GDPR (Article 12)**. Policy changes should be immediately updated and expired links removed; for example, data subjects asking for the deletion of non-users data are suggested to contact WhatsApp via the contact's form but the form no longer exists [23]. A practical approach would be to provide privacy dashboards and pictograms outlining the essence of a privacy policy, along with comprehensive instructions on how users can opt out of sharing certain information with WhatsApp.

5. Restrict data collection and retention to the absolute essential

Minimization of personal data can be achieved by collecting data of less people, or collecting less data of people. Only necessary data should be collected and used for the intended purposes, while redundant data, especially those obtained from non-users should be abandoned. WhatsApp should also focus on local data processing to reduce the amount of data stored in their online servers. For example, usage logs should be stored locally on users' devices. Utilize opt-in (no processing without prior consent) rather than opt-out (processing occurs unless consent is revoked later).

7 Conclusion

This report aims to systematically examine WhatsApp by applying the LINDDUN privacy threat modeling methodology. By mapping each element from Data Flow Diagram, we detected 30 threats and found 3 technical risks, 5 legal risks, and 4 ethical risks.

We believe the Privacy-by-design and Privacy-by-default paradigms are the two GDPR fundamentals that WhatsApp should embrace more actively to meet legal requirements and enable a more transparent and trusting relationship between WhatsApp and the users. The suggestions we formulated in the report are primarily based on these key principles.

References

[1] Cosette Cressler. *Understanding WhatsApp's Architecture System Design*. 2020. URL: https://www.cometchat.com/blog/whatsapps-architecture-and-system-design (visited on 10/12/2021).

[2] Kasun Dissanayake. *Whatsapp System Design and Chat Messaging Architecture*. 2020. URL: https://kasunprageethdissanayake.medium.com/whatsapp-system-design-and-chat-messaging-architecture-part-1-29fb4f0d14af (visited on 07/24/2020).

[3] *European Data Protection Supervisor*. 2022. URL: https://edps.europa.eu/data-protection/data-protection/glossary/d_en#data_minimization.

[4] WhatsApp's FAQ. *About end-to-end encryption*. 2021. URL: https://faq.whatsapp.com/820124435853543.

[5] WhatsApp's FAQ. *What information does WhatsApp share with the Meta Companies?)* URL: https://faq.whatsapp.com/1303762270462331 (visited on 12/31/2022).

[6] LINNDUN framework. *LINDDUN tutorial*. URL: https://www.linddun.org/downloads (visited on 12/31/2022).

[7] James Frew. *Is WhatsApp Safe? 5 Scams, Threats, and Security Risks to Know About*. 2022. URL: https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/.

[8] Mike Isaac. *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*. URL: https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html (visited on 12/31/2022).

[9] WhatsApp's Legal. *Information for people who don't use WhatsApp*. URL: https://www.whatsapp.com/legal/information-for-people-who-dont-use-whatsapp/?lang=en (visited on 12/31/2022).

[10] Claire Morrissey. *Data Protection: Key Findings from the EDPB's WhatsApp Ireland Decision*. 2021. URL: https://maples.com/en/knowledge-centre/2021/9/data-protection-key-findings-from-the-edpbs-whatsapp-ireland-decision.

[11] WhatsApp Privacy Policy. 2021. URL: https://www.whatsapp.com/legal/privacy-policy (visited on 04/01/2021).

[12] WhatsApp's Privacy Policy. *Information We Collect*. URL: https://www.whatsapp.com/legal/privacy-policy-eea/?lang=en#privacy-policy-information-we-collect (visited on 12/31/2022).

[13] General Data Protection Regulation. URL: https://gdpr-info.eu/ (visited on 12/31/2022).

[14] General Data Protection Regulation. *Art 12. GDPR: Transparent information, communication and modalities for the exercise of the rights of the data subject.* URL: https://gdpr-info.eu/art-12-gdpr/ (visited on 12/31/2022).

[15] General Data Protection Regulation. *Art 17. Right to erasure ('right to be forgotten').* URL: https://gdpr-info.eu/art-17-gdpr/ (visited on 12/31/2022).

[16] General Data Protection Regulation. *Art 25. Data protection by design and by default.* URL: https://gdpr-info.eu/art-25-gdpr/ (visited on 12/31/2022).

[17] General Data Protection Regulation. *Art 4. GDPR: Definitions.* URL: https://gdpr-info.eu/art-4-gdpr/ (visited on 12/31/2022).

[18] General Data Protection Regulation. *Art 5. GDPR: Principles relating to processing of personal data.* URL: https://gdpr-info.eu/art-5-gdpr/ (visited on 12/31/2022).

[19] Signal. *WhatsApp's Signal Protocol integration is now complete.* URL: https://signal.org/blog/whatsapp-complete/.

[20] *The General Data Protection Regulation and the WhatsApp Problem of Enterprises.* 2020. URL: https://teamwire.eu/en/the-general-data-protection-regulation-and-the-whatsapp-problem-of-enterprises/ (visited on 01/05/2020).

[21] *The right to be informed (transparency) (Article 13 14 GDPR).* 2022. URL: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-.

[22] *Understanding the 7 Principles of the GDPR.* 2021. URL: https://www.onetrust.com/blog/gdpr-principles/.

[23] WhatsApp. *Contact Forms.* URL: https://www.whatsapp.com/contact/forms/175626068100131/.

[24] WhatsApp. *WhatsApp's Privacy.* URL: https://www.whatsapp.com/privacy.

[25] *WhatsApp issued second-largest GDPR fine of €225m.* 2021. URL: https://www.bbc.com/news/technology-58422465 (visited on 02/09/2021).