INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

WhatsApp Data Policy, Data Security and Users' Vulnerability

Oluwaseun Oladeji Olaniyi
Information Technology Researcher, School of Computer and Information Sciences,
University of the Cumberlands, USA
Dagogo Sopriala Omubo
Researcher, Well Engineering and Information Technology,
Shell Petroleum Development Company, Nigeria

Abstract:
Several regulatory agencies regulate companies that deal with users' data, but specifically in the UK, they are regulated by the European Union General Data Protection Regulation (GDPR). The techniques of handling and processing data, rights of users, sanctions for defaulters, and other regulating clauses are formulated and implemented by these agencies to minimize the exploitation of the masses. Data regulation and management are essential because companies managing users' data are expected to handle data with care, caution, and due diligence. However, WhatsApp (arguably the most powerful instant messaging application in use) has been involved repeatedly in several cases that compromised the security of its users' data over the years. The platform has become a prime target and medium for predators (con artists, fraudsters) with intentions to access users' data (phone numbers, last seen, live location, and others) for vile purposes. These cases include leaked data that could be used for marketing purposes, phishing, impersonation, and fraud. This paper highlights recent cases of data security (data leakages) and privacy policies involving WhatsApp, examining the various issues that threaten WhatsApp users and make them vulnerable to exploiters, cybercrime, and con artists. It also considers how WhatsApp can protect its users against vulnerabilities. Also, the European Union GDPR was examined in line with WhatsApp's privacy policy to measure compliance with the regulation in light of recent data breaches.

Keywords: *Con artists, data breach, encryption, privacy policy, vulnerabilities, WhatsApp*

1. Introduction

Social media platforms are fast becoming an effective means of communication globally (Obar et al., 2015; Miller et al., 2016; Abdulmohsen et al., 2021). These platforms have enabled individuals and organizations in various countries to communicate and helped them build a social network and relations (Obar et al., 2015). Abdulmohsen et al. (2021) assert that there was a 9% global average penetration increase rate in the use of social media post-covid 19 eras. WhatsApp (arguably the leading messaging application globally) is presently used by over two billion people across over hundred and eighty (180) countries (WhatsApp, 2023). The application has helped many people stay in touch with family and friends anywhere and anytime. The application provides free communication services to its users, with a simple and user-friendly interface and features that make the platform convenient and essential for users (WhatsApp, 2023). The vitality of WhatsApp's communication service and the quality of value that it offers users for free is commendable. However, it is also suspicious, as the company has been involved in several data privacy policy and security issues that have attracted severe scrutiny in the past few years (Tamori et al., 2018). Cases such as the availability and publicity of users' data on hackers' forum and the dark web, the outage of the WhatsApp platform for about six hours, formulation of policies that reduce users' control and choice or denies users the opportunity to opt out, are some of the many challenges that WhatsApp usage attracts in recent times. In 2021, WhatsApp was fined by the Irish data protection watchdog (Ireland Data Protection Commission), after which it was also instructed to change its policies (BBC, 2023). The company was fined due to the investigation results (which lasted for almost a year), revealing that WhatsApp is not transparent enough about handling user databases. Such data compromise cases have prompted millions of users to seek an alternative to WhatsApp by switching to other messaging apps, such as Signal, Telegram, and others. This article critically examines WhatsApp as a company and its users' data security concerning its privacy policies. The vulnerabilities that users' data are liable to, WhatsApp data security and privacy policy cases, and the European Union GDPR are all explored, focusing on WhatsApp.

2. Overview of WhatsApp

WhatsApp was launched in 2009 by Brian Acton and Jan Koum (former employees of Yahoo) and was later acquired by Facebook 5 years later, in 2014 (Baulch et al., 2020; Bajaj & Jindal, 2015). According to Sevitt (2017), WhatsApp is today's most preferred telecommunication application. Generally, WhatsApp enables users to communicate via sending and receiving pictures, messages, voice notes, videos, and even calls (Baulch et al., 2020). The success enjoyed

by WhatsApp across the globe cannot be categorically traced to one factor. Some users (especially in rural areas) prefer WhatsApp to other applications as it allows them to communicate without limitations, unlike some social media platforms (Tapsell, 2018). According to Pereira and Bojczuk (2018), WhatsApp's appeal lies in its cost-effectiveness as an alternative to SMS and calls for some users. Urban middle-class users are drawn to its unique features, such as group messaging, encryption-based security, and privacy.

According to Endeley (2018), encryption is coding text information into scrambled and unreadable characters through a unique key that only the intended recipient can decode using their unique secret key to decipher the message. WhatsApp introduced encryption of messages into its features in 2016 to guarantee and cultivate a sense of trust and security of data in the users' minds (Zanon, 2018). This move follows the attacks on other applications, which led to the leakage of users' information that compromised privacy (Zanon, 2018). Some studies assert that communication platforms that feature end-to-end encryption should be considered safe compared to others that do not have such security features so that any information can be shared, and there is a guarantee that such conversations are safe (Khazraee & Losey, 2016; Dencik et al., 2016; Hintz et al., 2019). Before WhatsApp implemented encryption, the data contained by the WhatsApp database was vulnerable and could be accessed quickly, which entails a third party gaining complete conversation details. This motivated WhatsApp officials to fortify data security by encrypting it (Sahu, 2014). However, despite WhatsApp's end-to-end encryption, the application is still open to some issues that compromise users' data, which suggests that the company does not prioritize users' data security over its profitability, as some users' data are still sharable to third parties (Zanon, 2018; Santos & Faure, 2018). Despite the use of end-to-end encryption, which is intended to enhance the security of messages and call conversations, there remains a possibility of susceptibility to attacks, especially in the event of a breach on either end of the communication (Wijnberg et al., 2021; Rosler et al., 2018; Agarwal et al., 2022). As such, WhatsApp users may still be vulnerable to data and privacy breaches, as highlighted by previous studies (Rosler et al., 2018; Dechand et al., 2019; Seamons, 2022).

3. Review of WhatsApp Data and Privacy Policies

Like every company has a privacy policy related to users' data, WhatsApp also has its data policies (Gol et al., 2019). A privacy policy is a system that allows companies to request the permission of users' data and their consent to some data processing using the data that has been and will be entered into the company's application or website (Gol et al., 2019). Gol et al. (2019) noted that privacy policies are typically formulated, dictated, or crafted by the service provider. WhatsApp Inc (2023) acknowledges that its privacy policy aims to inform users about the company's policies and their data or information usage. This policy gives users an understanding of how their information is utilized, processed, and protected through a detailed explanation of the measures taken to safeguard their privacy. These policies can be found in the company's terms of service and privacy policy for all its users.

WhatsApp emphasizes that users' information must be collected for the company to operate, improve support, and market its services (Zingales, 2017). The data collection process is automatic such that if users are unwilling to provide the requested information, they cannot access the services they need (Zingales, 2017; WhatsApp Inc, 2023).

The following is some of the information required from users of WhatsApp services and how they are treated in the privacy policy:

- Account information: In order to use the WhatsApp services, there is a need to create a WhatsApp account which will require the potential user's phone number, a name, and a picture (WhatsApp Inc, 2023).
- User's messages: Messages or conversations of the users are not retained during the service; instead, they are stored on the user's device after they have been delivered and not to the company's server (WhatsApp Inc, 2023). However, WhatsApp will keep user's messages in the following situations:
- Undelivered messages: When messages are not delivered to recipients, they are encrypted for 30 days, after which they are deleted.
- Forwarding of media: When forwarded, they are stored in an encrypted format on the company's server to enhance efficiency when forwarded (WhatsApp Inc, 2023).

Some of the following is information automatically collected from every user that uses the services of WhatsApp:

- Log and usage information: Information about the user's activity is usually collected automatically, data such as settings, features used, frequency of service use, calls, status, last seen, etc. (WhatsApp Inc, 2023).
- Device and connection information: Information regarding the user's device is usually collected when installing and using the application or web-based services. Such information includes the device's operating system, battery level, mobile network, hardware model, language, time, phone number, etc. (WhatsApp Inc, 2023).
- Location information: Users are usually asked to turn on their locations to serve customers better, especially when there is a need for troubleshooting or diagnosis; users' IP addresses and area codes from phone numbers are used to deduce the user's location (WhatsApp Inc, 2023).
- Cookies: Cookies are used to improve the experience of users who want to use the web-based services; this will, however, require more information from the user; the user's data will be tracked to know how best to serve such customers (WhatsApp Inc, 2023).
- Third-Party Information: Information about a user is usually garnered from various means. Users can grant third parties access to their accounts or information on WhatsApp if they so desire the services of such third parties. Users can grant permission to third parties to access their data, like phone numbers, names, and other information shared with Whatsapp (Whatsapp Inc., 2023). The company requires that such users have the correct and such information (WhatsApp Inc, 2023). Also, the third-party information is obtainable from 'user reports,'

and in such situations, information about the person making the report and the person who is reported is collected (WhatsApp Inc, 2023).

4. How WhatsApp Uses Collected Information

WhatsApp uses the information gathered directly and automatically from users alongside the ones collected from third parties for specific purposes. The data are used to provide quality and customized services to users and good customer service (WhatsApp Inc, 2023). The same information collected from users will also be used to improve the company's services and test new features that will give users the best experience. Secondly, the information gathered is also used to provide security to users against harmful activities such as hacking a user's account, spam, and even online stalking; this is used to verify users' accounts and actions (WhatsApp Inc, 2023). Furthermore, the information gathered is used to propose business interaction with third parties using features such as catalogs, allowing potential buyers to go through the goods or services provided by the user's business and place their orders (WhatsApp Inc, 2023). Finally, WhatsApp pointed out that it has the proper and legal backing to enforce its terms and conditions of service and its privacy policy on its users and any other affected party and also carry its investigation on any person from whom it suspects violations against its policies while also protecting the user's right, data and safety (WhatsApp Inc, 2023).

In light of the preceding, Kalyani (2022) alludes that the provision that users' data can be shared with the parent company and other subsidiaries as well as with third parties for commercial purposes is a primary concern of every WhatsApp user who makes use of the "FREE" services because their data could be the actual cost of so-called free services. However, according to the GDPR of the European Union, service providers should make the processing of end-users data transparent in a comprehensible way (Gol et al., 2019). In addition, Gol et al. (2019) assert that service providers are responsible for granting end-users control over their data, and privacy policies should be concise enough to enable users to understand how their data has been processed and comprehend the policy in its entirety.

5. WhatsApp Data Security and Cases

In the past few years, WhatsApp has faced issues from different user categories regarding its privacy settings and the security of user data, such as phone numbers. Jurgita (2023) outlines in a news article published on cybernews that an actor advertises the sales of four hundred and eighty-seven (487) million WhatsApp users' phone numbers on a popular hacking forum. The database contains data from eighty-seven (87) different countries that use WhatsApp, including the United States of America, Egypt, Italy, Saudi Arabia, Turkey, France, and others (Jurgita, 2023). The thought that this information (no matter how insignificant phone numbers are considered) in such large quantity is on sale is disturbing, as it is detrimental to millions of WhatsApp users and is being sold at a considerable price. It is worth noting that these little acts, as insignificant as they might seem, have grave consequences. Jurgita (2023) affirms this detriment, highlighting that minute information like active phone contacts is used for smishing and vishing attacks; thus, the users whose contacts are on the database are not safe.

In research conducted to verify the validity of the phone numbers, Cybernews network confirmed that the numbers provided from the database sample were active WhatsApp users' phone numbers. The means through which the data was acquired has not been revealed. However, such data is obtainable through a hacking process known as scraping (Wong, 2022). Jurgita (2023) argues that Meta Inc. (the parent company of WhatsApp) has a history of tolerating third-party scraping activities to access users' data of its services.

In another similar case, this time involving data leaks of Facebook users, including names, phone numbers, and other personal details, the database of over 530 million people were publicly available (Tidy, 2021; Yadav, 2022; Wong, 2022). This data leak is also detrimental to WhatsApp users as the details include phone numbers likely to be the WhatsApp numbers of Facebook users, as the social media platform is also owned by Meta (which also owns Whatsapp). Meta has refuted the allegations of a recent data breach, stating that the data extracted is from an older leakage as opposed to being the result of a recent attack (Tidy, 2021). However, while Facebook's explanation that the data is from a prior leak does not explicitly acknowledge that the phone numbers may belong to current WhatsApp users, the probability of this occurrence remains high, given that Facebook and WhatsApp are both owned and operated by Meta. Additionally, WhatsApp's privacy policy permits sharing of user data with other subsidiaries, including Facebook (WhatsApp, 2021).

Tidy (2021) asserts that it is worth noting that these details are not just leaked, but they are also published in hacking forums, making users more vulnerable and susceptible to harm. Tidy (2021) further stressed that issues like this are familiar to companies with large databases, and it is becoming a trend. Companies should not just continue to say they have 'fixed the issues' after the data has been leaked because these leaks have an extended impact on users, especially those who are not cyber-conscious. Thus, appropriate measures should be taken to safeguard users' data and keep them safe from fraudsters or con artists. Security experts allude that the leaked data are more likely to be used for targeted attacks on WhatsApp users, highlighting the ripple effects of these cases (Tidy, 2021).

6. Impacts of Data Leaks on Users

The victims of these data leaks and privacy compromises suffer severe losses in various forms, which may result in regret for such users. Dearden (2022) reports the case of a victim (Sarah Capper) whom scammers targeted due to a leaked phone number. The victim continued receiving text messages from con artists who requested money after claiming to be her family member. Some of the messages contained endearments associated with close family members like 'Hello mum,' 'Hello dear,' 'I have gotten a new number, please save it,' etc. (Dearden, 2022). Another victim Zoe Burell was contacted by an unknown number impersonating her daughter and requesting money after she was asked to delete the old number and save the new one. Burell did not view the request as harmful, as her daughter had changed phone numbers

multiple times and had previously borrowed money from her. These messages will look harmless and genuine to someone who is not used to the tactics of these cyber criminals/ fraudsters or who is not cyber-conscious. The leakages of data have cost people a lot, even financially. The police mentioned that each person being scammed loses an average of two thousand five hundred pounds to these con artists (Dearden, 2022).

In reacting to the scam and leakages of WhatsApp users' phone numbers, Karthryn Harnett from WhatsApp said that any user who receives such messages should do their due diligence by calling or requesting a voice note from the person sending such messages.

Does WhatsApp trade users' data for financial gains? According to Kleinman (2021), WhatsApp's updated terms and conditions (which include giving WhatsApp the autonomy to use their data without prior permission) left users no option, as they were automatically denied the service of WhatsApp. This denial of service to users who refuse to agree to its privacy policy is a source of suspicion and concern, considering that the service is rendered accessible. Arguably, vulnerability and relinquishing rights to data are the price users must pay to use WhatsApp's services. The users' immediate response was to seek alternatives such as Signal and Telegram.

Another case that could cause discomforting thoughts for users of the application is the pressure by the government of countries on WhatsApp to allow them access to users' data. According to BBC News (2021), WhatsApp claims that it receives pressure from the government in the UK to compromise its end-to-end encryption to open access to regulating government agencies in instances of investigation. This will make users' messages, shared files, pictures, videos, and others accessible to third parties.

However, in contrast, WhatsApp criticizes the request, stating it stands against government pressure to compromise its end-to-end encryption. WhatsApp further stressed that the government is supposed to demand strong security rather than encourage weak security from tech companies. Issuing a statement in defense of its security, WhatsApp affirms that the company would stop providing services in the UK if it is required by the government to weaken the privacy of its encrypted messaging system (Kleinman, 2022).

Meta acknowledges that users' data is being targeted by malicious activities on its various platforms, including WhatsApp. The company further asserts that certain surveillance firms are engaged in such illicit activities. It is then plausible to say that users of WhatsApp, despite its end-to-end encryption, are still liable to suffer attacks due to data sharing to WhatsApp. It is noteworthy that WhatsApp was fined a sum of two hundred and twenty-five million euros (€225m), an equivalent of one hundred and ninety pounds (£190m) by the Irish data protection watchdog (the second largest fine issued in the history of GDPR) after which it was also directed to change its policies (BBC, 2023). WhatsApp was fined because the investigation results (which lasted for almost a year) on the company revealed that it is not transparent enough about handling users' databases. Also, in 2021, Meta's key platforms, Facebook, Instagram, and WhatsApp, suffered an outage, making the services inaccessible for over six hours (Shead, 2021). The company expressed regret for the outage, clarifying that they were unaware of the cause and reassuring users that no user information had been compromised. Nevertheless, the company advised users to consider changing their passwords for those affected accounts (Shead, 2021). Despite all these, WhatsApp maintains that users' chats are encrypted end-to-end. None of its policies, including the new terms and conditions recently updated, allows for third-party access, except for other Meta subsidiaries (WhatsApp, 2022).

6.1. WhatsApp vs. EU's GDPR Policy

The European Union GDPR was adopted in 2016 to replace the Data Protection Directive (DPD) to unify the data protection standards amongst countries and facilitate cross-border data transfer. The GDPR of the European Union is widely regarded as the most robust framework for safeguarding the privacy and security of personal data about European citizens, regardless of whether the data is collected within or outside the EU (Voigt, 2017; European Council). The regulation, which came into effect on May 25, 2018, aims to provide citizens with greater autonomy over the collection, processing, and protection of their data by organizations (GDPR, 2023).

The GDPR is a policy that guides how individual data are processed; it ensures that companies comply with the standards set and that any breach of rules is sanctioned. This regulation guides companies that deal with the data of individuals transacting with them and explains such individuals' rights. This will, in turn, help individuals to be more aware of their data rights and give them control over their data. The GDPR offers guidelines on how to handle the following:

- Individuals' fundamental rights in the digital age
- The obligations of companies processing data
- The methods for ensuring compliance with the set standards
- Sanctions for companies breaching the standards or rules (European Council)

The GDPR obligated businesses and organizations to take appropriate measures to ensure customer data safety. Meta's companies, including Facebook and WhatsApp, have been alleged to have cases of compromise with this law, as there have been several cases of leaked user data such as phone numbers, locations, and other information that makes users vulnerable to cyber victimization and scam incidents (Dearden, 2022). However, in one of the statements WhatsApp released to address the recent six hours outage, the company claimed that they are unaware of the issue and can guarantee that no users' data was breached or compromised (WhatsApp, 2022). WhatsApp also recently updated its terms and conditions globally but exempted those living in a country or territory listed amongst the European Region. WhatsApp Ireland Limited provides services to users within this category. It means that WhatsApp Ireland Limited provides users' data within this region. Any other users besides those in the abovementioned category are served by WhatsApp LLC (WhatsApp, 2022).

Also, WhatsApp was fined by Ireland's Data Protection Commission for violating the European Union's GDPR. This was because WhatsApp was found guilty of not being transparent in handling its users' data. Sufficient information was not provided regarding data collection (Bateman, 2021). The Irish regulator who issued the fine has also called WhatsApp to order by asking it to carry out some remedial actions on its data processing.

Considering the preceding, it is arguable that WhatsApp truly falls short of the policies and provisions of the EU's GDPR. Hence, it has made provisions to cover these shortcomings through its subsidiary (WhatsApp Ireland Limited), which will now manage the services of WhatsApp for EU citizens. It is then plausible to say that WhatsApp LLC does not manage users' data optimally, at least in the context of the EU's GDPR. This is likely a concern for WhatsApp users outside the EU, as their data will still not be managed optimally since WhatsApp has adopted different strokes for different folks' approaches. If WhatsApp insists on adopting the GDPR for only EU users, and will not adopt a similar policy for users in other regions, then there must be some benefits it derives from non-compliance to such standards; hence WhatsApp users must be aware and not totally trust WhatsApp with sensitive data or even rely on the company for total protection of its data.

6.2. WhatsApp Users' Vulnerabilities

The data of the users of WhatsApp Messenger are end-to-end encrypted, as discussed beforehand, which means that it is limited to surveillance. Still, ambiguous user database exposes it to attack (Bogos et al., 2023), and Point (2023) identified some noticeable leakage in data protection. For instance, Bogos et al. (2023) found that hackers may exploit users' vulnerability and feed on their data maliciously simply by sending them a seemingly innocent vCard containing malicious codes. These hackers use this code mainly to exploit the WhatsApp web, and after opening the file, the attached arbitrary code runs on the computer and leaves it in a compromising state for hackers to have full access to the user's data (Bogos et al., 2023; Point, 2023). The hackers rely on the fact that users of WhatsApp can view any media or attachment, thereby exploiting that vulnerability.

Bogos and colleagues (2023) assert that the WhatsApp policy for offline backups has created a vulnerability that allows attackers to obtain encrypted data. In a study on Android WhatsApp forensics conducted by Thakur (2013), it was discovered that the encrypted database could be extracted using a Universal Forensic Extraction Device (UFED) physical analyzer. The extracted data can then be organized in a Hypertext Markup Language (HTML) format using Xtract 2.0, facilitating easy understanding. Conclusively, Thakur (2013) asserts that The Advanced Encryption Standard (AES) cipher implementation on Android made it easy to access the database, which consists of all the necessary data of the users. Although this loophole may have been rectified, it still points out that hackers are constantly identifying and researching means through which WhatsApp users can become vulnerable and exploited.

According to Bogos et al. (2023), WhatsApp utilizes an open and freely accessible protocol called Extensible Messaging and Presence Protocol (XMPP). This protocol facilitates the exchange of communication between clients and supports data transmission from one endpoint to another. XMPP is primarily employed for instant messaging and provides online presence notification during active conversations. Extensible messaging and presence protocol is an open standard protocol used by WhatsApp in a modified manner that can be operated on mobile devices at low-bandwidth networks (Bogos et al., 2023). Based on the fact that extensible messaging and presence protocol (XMPP) is an open standard, therefore giving room to any developer to access the protocol, wherefore creating a server that might affect the other servers and leaving WhatsApp communication vulnerable (Bogus et al., 2023).

It is also plausible to state that data ambiguity relatively influences WhatsApp users' data vulnerability. The large number of users on WhatsApp has created a more extensive database, which, if not adequately protected, attracts more significant attacks (Bogos et al., 2023). Additionally, the usage policy is also essential to note; the emphasis is on the fact that it is owned by Facebook, which allows data collection and usage practices. Despite the encryption, Facebook still has access to the data, which has become a concern for WhatsApp privacy. (Baulch et al., 2020; Bogos et. al., 2023).

7. Recommendations

Mirza et al. (2020) assert that it is not typically advised to save messages on a platform that is not encrypted. Although WhatsApp has some control to protect users' data, such as security notifications, end-to-end encryption, and two-step authentication PIN. However, this will not guarantee WhatsApp or the platform's users are safe from third-party attacks, nor will it resolve the issues WhatsApp faces. This study recommends implementing additional security measures to address the concerns raised and the limited security checks currently provided by WhatsApp. It also suggests that WhatsApp should enhance user access control and address communication risks to improve security. Although WhatsApp operates an accessible model for the services offered to users, we recommend that the company provides free services to all users and also designs a premium service whereby users can choose their settings, decide to either give permission or decline the usage of their data, and be guaranteed privacy with their data on the WhatsApp platform.

8. Conclusions

WhatsApp clearly has some limitations and poses some vulnerabilities to platform users. Users may have some control over their applications' security and privacy settings. Still, in reality, platform settings are made to safeguard the platform owner, not the business data of end users. This does not suggest that companies using WhatsApp for communication and advertising should stop using them. For example, in the case of businesses using WhatsApp for commercial communication across broader international markets, doing so could cut them off from many clients. WhatsApp security problems expose companies to potential data breaches, which can have an even more significant adverse effect on their bottom line. Hence, users are advised to play their part in safeguarding their data by taking

preventive measures, such as ensuring that the app is always up to date and becoming more cyber-conscious to protect themselves against cyberattacks such as smishing, vishing, phishing, and the like.

9. References

i. Abdulmohsen S. A. & Thamer A. (2021). Evaluating and comparing the usability of privacy in WhatsApp, Twitter, and Snapchat. *International Journal of Advanced Computer Science and Applications,* Vol. 12(8), 251–259.
ii. Albesher, A.S. and Alhussain, T., (2021). Evaluating and comparing the usability of privacy in WhatsApp, Twitter, and Snapchat. *International Journal of Advanced Computer Science and Applications,* vol.12 (8) pg. 1–9.
iii. Andysah S., Utama P., Robbi R., Solly L., Hardianto D., Nuning K. & Andika B. (2018). Insecure Whatsapp Chat History, Data Storage, and Proposed Security.
iv. Anju T., Bhujade, Rakesh B., & Amit S. (2018). Analysis of WhatsApp security.
v. Bajaj, H. and Jindal, R., (2015). Thinking beyond WhatsApp. *International Conference on Computing for Sustainable Global Development* (INDIACom), pp. 1443–1447.
vi. Bateman, T. (2021). WhatsApp rewrites its Europe privacy policy after a record €225 million GDPR fine. *Euronews.*
vii. Baulch, E., Matamoros-Fernández, A. and Johns, A., (2020). Introduction: Ten years of WhatsApp: The role of chat apps in the formation and mobilization of online publics. *First Monday.*
viii. BBC News. (2019). Why India wants to track WhatsApp messages.
ix. BBC News. (2021). Instagram and WhatsApp outage: What Facebook's apology really said.
x. BBC News. (2021). Meta bans surveillance-for-hire firms for targeting users.
xi. BBC News. (2021). WhatsApp and Facebook to share users' data outside Europe and UK.
xii. BBC News. (2021). WhatsApp blocks two million Indian accounts.
xiii. BBC News. (2021). WhatsApp privacy policy tweaked in Europe after record fine.
xiv. BBC News. (2021). WhatsApp: Facebook-owned app goes to court over India privacy rules.
xv. BBC News. (2023). WhatsApp issued the second-largest GDPR fine of €225m.
xvi. Bogos C. E., Mocanu R. & Simion E. (2023). A security analysis comparison between Signal, WhatsApp, and Telegram *International Association for Cryptologic Research.*
xvii. Bogos, C.E., Mocanu, R. & Simion, E., (2023). A security analysis comparison between Signal, WhatsApp, and Telegram. *Cryptology e-Print Archive.*
xviii. Cybernews, (2022).
xix. Dearden, B. C. (2022). WhatsApp: Scam costs Welsh victims thousands of pounds. *BBC News.*
xx. Dencik L., Hintz, A., & Cable J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*.
xxi. Dev, J., Das, S. and Camp, L.J., (2018). Privacy practices, preferences, and compunctions: WhatsApp Users in India. Pp. 135–146.
xxii. Endeley, R.E., (2018). End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security,* Vol. 9(1), p.95.
xxiii. Gol Mohammadi, N., Leicht, J., Ulfat-Bunyadi, N. and Heisel, M., (2019). Privacy policy specification framework for addressing end-users' privacy requirements. In trust, privacy, and security in digital business. *Springer International Publishing,* pp. 46–62.
xxiv. Hintz A. Dencik L. & Wahl-Jorgensen K. (2019). Digital citizenship in a datafied society. *Cambridge: Polity Press.*
xxv. http://globalmedia.mit.edu/2018/11/09/zap-zap-whos-there-whatsapp-and-the-spread-of-fake-news-during-the-2018-elections-in-brazil/.
xxvi. https://cybernews.com/news/whatsapp-data-leak/
xxvii. https://cybernews.com/news/whatsapp-data-leak/#comments
xxviii. https://doi.org/10.1177/186810341803700302.
xxix. https://doi.org/10.1177/2053951716679678
xxx. https://doi.org/10.1177/2056305118795876.
xxxi. https://doi.org/10.1177/2057047315625076
xxxii. https://doi.org/10.14324/111.9781910634493
xxxiii. https://doi.org/10.31227/osf.io/2sbfc.
xxxiv. https://gdpr.eu/companies-outside-of-europe/#:~:text=The%20GDPR%20does%20apply%20outside,%E2%80%9Cextra%2Dterritorial%20effect.%E2%80%9D
xxxv. https://medium.com/@gzanon/no-end-to-end-encryption-does-not-prevent-facebook-from-accessing-whatsapp-chats-d7c6508731b2, accessed March 15, 2023.
xxxvi. https://soyacincau.com/2022/11/29/whatsapp-data-breach-meta-denies-500-million-phone-numbers-report-speculative/
xxxvii. https://theprobe.in/stories/the-whatsapp-privacy-policy-saga-indias-data-protection-regime-and-you/
xxxviii. https://www.bbc.com/news/newsbeat-58803953
xxxix. https://www.bbc.com/news/technology-55573149
xl. https://www.bbc.com/news/technology-55634139
xli. https://www.bbc.com/news/technology-56154543

xlii. https://www.bbc.com/news/technology-56639081
xliii. https://www.bbc.com/news/technology-57440405
xliv. https://www.bbc.com/news/technology-58422465
xlv. https://www.bbc.com/news/technology-59348921
xlvi. https://www.bbc.com/news/technology-59692240
xlvii. https://www.bbc.com/news/technology-64863448
xlviii. https://www.bbc.com/news/uk-wales-60243593
xlix. https://www.bbc.com/news/world-asia-india-50167569
l. https://www.bbc.com/news/world-asia-india-57251612
li. https://www.bbc.com/news/world-asia-india-57831201
lii. https://www.bloomberg.com/profile/company/0350539Z:US?leadSource=uverify%20wall
liii. https://www.cnbc.com/2021/10/05/facebook-says-sorry-for-mass-outage-and-reveals-why-it-happened.html
liv. https://www.cnbctv18.com/technology/another-cybersecurity-firm-alleges-whatsapp-data-leak-15329791.htm
lv. https://www.euronews.com/next/2021/11/22/whatsapp-rewrites-its-europe-privacy-policy-after-a-record-225-million-gdpr-fine
lvi. https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html#:~:text=Meta%20Fined%20%24414%20Million%20After,Law%20%2D%20The%20New%20York%20Times
lvii. https://www.similarweb.com/blog/popular-messaging-apps-by-country
lviii. https://www.spiceworks.com/it-security/data-security/news/whatsapp-alleged-data-leak/amp/
lix. https://www.whatsapp.com/legal/privacy-policy/?lang=en
lx. Jurgita, L. (2023). WhatsApp data leaked - 500 million user records for sale online. *Cybernews*.
lxi. Kalyani, P. (2020). An empirical study on Whatsapp privacy policy, analyzing the actual cost of free apps in an online social network in contrast to other players like Telegram, Signal, etc.
lxii. Kamide G. (2022). Overcoming WhatsApp security risks and compliance concerns. *SafeGuard Cyber.*
lxiii. Khazraee E. & J. Losey J. (2016). Evolving repertoires: Digital media use in contentious politics. *Communication and the Public*, vol.1 (1), 39–55.
lxiv. Kleinman, B. Z. (2021). WhatsApp launches privacy campaign after backlash. *BBC News.*
lxv. Kleinman, B. Z. (2021). WhatsApp to switch off messages for all who reject new terms. *BBC News.*
lxvi. Kleinman, B. Z. (2021). WhatsApp users flock to rival message platforms. *BBC News.*
lxvii. Koh, You Liang. (2018). Investigating Potentially Harmful Applications on Android.
lxviii. M. B. Leahy & S. J. Sablan (1990). Multiple model-based controls of robotic manipulators: theory and experimentation. *International Symposium on Intelligent Control*, Vol. (2) Pg 830–835.
lxix. M. Santos & A. Faure, (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption, Social Media + Society.
lxx. Miller, D., Elisabetta, C., Haynes, N., McDonald, T., Nicolescu, R., Sinanan, J., Spyer, J., Venkatraman, S., & Wang, X. (2016). How the World Changed Social Media.
lxxi. Mirza. M. M. Salamh F. E. and Karabiyik U. (2020). An android case study on technical anti-forensic challenges of WhatsApp application. *International Symposium on Digital Forensics and Security (ISDFS),* Pg. 1–6, doi:10.1109/ISDFS49300.2020.9116192.
lxxii. Mishra, M. (2022). The WhatsApp Privacy Policy Saga: India's Data Protection Regime and You. *Latest News of India Today.*
lxxiii. Nagar, S. (2019). WhatsApp Hacking–A Wake-up Call for Users.GDPR 2023
lxxiv. Obar, J.A. & Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications Policy*, vol. 39(9), Pg. 745–750.
lxxv. Pereira G. & I. Bojczuk, (2018). Zap zap, who's there? WhatsApp and the spread of fake news during the 2018 elections in Brazil, *Global Media Technologies & Cultures Lab, MIT* at:
lxxvi. Point, C. (2023). WhatsApp Malicious card vulnerabilities allowed attackers to compromise hundreds of millions of WhatsApp users. *Global Security Magazine Online.*
lxxvii. Rastogi N. & James H. (2017). WhatsApp security and role of metadata in preserving privacy.
lxxviii. Sahu, MS, (2014). An analysis of WhatsApp forensics in Android smartphones. *International Journal of Engineering Research*, vol. 3(5), 349–350.
lxxix. Samuell C. Q., (2018). Data security and privacy in mobile technology: A case of Whatsapp. *Texila International Journal of Academic Research.* Vol. (5)1 Pg. 1–8.
lxxx. Satariano, A. (2023, January 4). Meta Fined $414 Million After Ad Practices Ruled Illegal Under EU Law. *The New York Times.*
lxxxi. Sevitt, D. (2017). The most popular messaging apps by country. *Similar Web*
lxxxii. Shead, S. (2021, October 5). Facebook says sorry for the mass outage and reveals why it happened. CNBC.
lxxxiii. Siahaan, A. P. (2018). Insecure Whatsapp chat history, data storage, and the proposed security. *International Journal of Pure and Applied Mathematics.* Vol. 119(16), 2481–2486.
lxxxiv. Siahaan, A.P., Rahim, R., Aryza, S., Djanggih, H., Kurniasih, N. and Buana, A.P., (2018). Insecure WhatsApp chat history, data storage, and the proposed security.

lxxxv. Tamori A., Bhujade R. K. & Sinhal A. (2018). Analysis of WhatsApp security. *International Journal of Ethics in Engineering & Management Education.* Website: www.ijeee.in, volume 5(6), Pg. 1–4.

lxxxvi. Tapsell, R (2018). The smartphone as the 'weapon of the weak': Assessing the role of communication technologies in Malaysia's regime change. *Journal of Current Southeast Asian Affairs*, volume 37(3) 9–29.

lxxxvii. Thakur, N.S., (2013). Forensic analysis of WhatsApp on Android smartphones.

lxxxviii. Tidy J. (2021). Facebook leak: Irish regulator probes "old" data dump. *BBC News.*

lxxxix. Vallance, B. S. (2023). WhatsApp: Rather be blocked in the UK than weaken security. *BBC News.*

xc. Voigt, P., and Von A. (2017). The EU General Data Protection Regulation (GDPR). doi:10.1007/978-3-319-57959-7

xci. Wadhwani, S., & Wadhwani, S. (2022, December 2). WhatsApp Leak: 360M Phone Numbers Freely Available on the Dark Web. *Spiceworks.*

xcii. WhatsApp Inc., (2023). WhatsApp Inc - Company Profile and News. Bloomberg.com.

xciii. WhatsApp privacy policy. (2021). Whatsapp.com.

xciv. Wong, A. (2022). Meta denies data leak involving nearly 500 million WhatsApp phone numbers; claims report was speculative.

xcv. Yadav, P. (2022, December 5). Another cybersecurity firm alleges WhatsApp data leak after denial by messaging app.

xcvi. Zanon, G. (2018). No, end-to-end encryption does not prevent Facebook from accessing WhatsApp chats. *Medium* at: