

REGULATORY

WhatsApp, a misconceived menace to society?

11 January 2021 9 min read

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice and member of Competition Law Practice; and Dale Adams, Candidate Legal Practitioner and Associate

Introduction

*"By tapping Agree, you accept the new **terms** and **privacy policy**, which takes 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."*^[1]

With these simple words, the Facebook-owned messaging giant, WhatsApp, sparked a public outcry concerning the recent update to its terms and privacy policy. The privacy policy update relates to how it processes the data of users, how businesses can utilise Facebook services to store their (business) chats and who partners with Facebook to offer integration across all Facebook products.

Users voiced displeasure about the app's changed policies are rife and social media relating to personal data/information being misused is increasing. Telegram users are also increasing by the minute!

However, is this switch justified? What is the exact situation with regard to the changes to WhatsApp and how concerned should people be?

WhatsApp security and privacy

WhatsApp is the largest messaging service in the world with over 2 billion monthly active users. Since its origins in 2009, WhatsApp has prided itself on its commitment to security and privacy with encrypted conversations and other important technologies integrated into the app.^[2] This is demonstrated by WhatsApp's latest privacy policy dated February 2021 which, amongst others, states that:

Your messages. *We do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers.*

In addition to the above, the WhatsApp privacy policy states that WhatsApp and other third parties cannot read the messages of its users due to the built in end-to-end encryption ("**E2E**"). Also, WhatsApp cannot decrypt the contents of a user's profile contents, that being messages, calls and photos.^[3]

This means that WhatsApp does not store personal information i.e. the content of your messages as such and delete your messages on their servers immediately.

What WhatsApp has access to is metadata, IP addresses, profile pictures, status updates and user contact information. Whilst metadata does not allow anyone to read a user's messages, it allows for transparency as to who and when a user messaged someone and for how long.^[4]

Telegram security and privacy

Telegram, an entity originally established in Russia with the aim of providing secure messaging, is the second largest messaging service in the world with over 400 million users. In the wake of Facebook's acquisition of WhatsApp in 2014, Telegram exponentially grew in popularity

purportedly due to its security and privacy features.[5]

Even though Telegram offers encryption on messages and other information, it is not enabled by default – like that of WhatsApp. The only way to use E2E encryption on Telegram is to use its “secret chats” feature.[6] In addition, the “secret chats” feature is only available for “chats” between two users. In theory, therefore, Telegram has access to your messages which are not covered by the veil of “secret chats” and they store this for 12 months.

Based on the above high level comparison of the security features utilised by WhatsApp and Telegram, it could be argued that WhatsApp’s security and privacy is more robust and secure than that of Telegram especially in that E2E encryption is a default feature.

So what personal information does Telegram have access to? In the Telegram Privacy Policy it is stated that Telegram processes, amongst others, the following set of personal information:

- basic account data such as user mobile number, profile name, profile picture and about information;
- user email addresses; and
- user messages in cloud chats such as messages, photos, videos and documents.

The above information goes further than the sets of personal information that WhatsApp has access to, and processes on behalf of its users, and WhatsApp by default provides E2E encryption.

Signal security and privacy

Several experts and users are encouraging people to move to Signal. Signal Messenger LLP, a US based and established social messaging platform, is considered the best alternative to both WhatsApp and Telegram from a security and privacy perspective.[7]

Like WhatsApp, Signal makes use of the open-source Signal Protocol to implement E2E encryption for communication on Signal. However, whilst WhatsApp encrypts messages and calls (which is sufficient for most users), Signal goes a step further and encrypts metadata as well. Furthermore, Signal also makes use of what is called “Sealed Sender”, which allows no one to be able to know – not even Signal – who is messaging whom.[8] This is but a small part of the Signal functionality. Other security features include, amongst others, passcode or biometrics lock and automatic face blur in messages.

Considering personal information Signal only stores a user’s phone number and nothing else.

The changes to the WhatsApp privacy

In essence, the new changes to WhatsApp terms and privacy policy relate to how WhatsApp will share information within the Facebook group of companies and how any shared information will be used. These key updates relate to:

- WhatsApp’s service and how it processes your data;
- how businesses can use Facebook hosted services to store and manage their WhatsApp chats; and
- how WhatsApp partners with Facebook to offer integrations across Facebook’s product portfolio.

It is important to note that the information collected by WhatsApp is not the “chats” of its users, as these are encrypted and therefore cannot be seen by the company. To the contrary, the information relates to personal data such as phone numbers of users (and their contacts, if the contacts make use of WhatsApp), profile names, pictures and diagnostic data.[9]

The updated privacy policy makes it clear on how WhatsApp will share data with the Facebook family of apps for better advertising targeting. [10] The fear is that this gives Facebook even more incentive to monetise user WhatsApp data. Statements have been made by many that the update of WhatsApp privacy policy will now enforce sharing of data from WhatsApp to Facebook and even that WhatsApp will completely invade user privacy. However, is this really the case?

WhatsApp has added new features to allow people to communicate with businesses – and those businesses could be hosted by Facebook. However, users should be informed if that happens by the specific business. When speaking to a business who has decided to have its messages managed by Facebook, a message should appear – and users should stop engaging with the specific business if they would prefer

that information not be managed by Facebook.[11] Businesses making use of the WhatsApp platform will be able to make use of Facebook services to store the business – customer chats.

Going forward, there will be an even greater integration between WhatsApp and Facebook's other products like Instagram and Messenger, but this means that they will share data like your phone number, transaction data,[12] IP address and information on how you interact with businesses.[13]

What exactly does this sharing of personal information between Facebook companies actually entail? The WhatsApp privacy policy states that this entails, amongst others:

- helping improve infrastructure and delivery systems;
- understanding how the WhatsApp or Facebook services are used;
- promoting safety, security and integrity across all Facebook company products;
- improving services and user experience such as personalising features and contents, helping users to complete purchases and transactions and showing relevant offers and advertisements across the Facebook company products; and
- providing integrations which enable users to connect WhatsApp with other Facebook company products. For example, allowing users to connect Facebook Pay account to pay for things on WhatsApp.[14]

So yes, advertising directed at a user specifically is possible and certain information will be shared to achieve that, but does Telegram differ in any significant way? That is doubtful.

In less detail, the Telegram privacy policy states that Telegram may share user personal data with their parent company, Telegram Group Inc. located in the British Virgin Islands and Telegram FZ-LLC, a group member located in Dubai to help provide, improve and support Telegram services. It has been reported that nearly eight years after its initial launch, Telegram needs to monetise its platform by either advertising or finding a buyer in order to ensure survival. The founder of Telegram, Pavel Durov, stated that the company will begin serving advertisements to cover some of its costs.

Conclusion

As businesses across the world prepare to re-open and expand online, people need simple ways to get in touch with businesses to ask questions, get information or find something they might buy. Today, WhatsApp supports more than 50 million WhatsApp business app users. In order to help them and the thousands of larger businesses on the WhatsApp business API get discovered, the company is introducing these new features to start a chat with a business on WhatsApp to see what goods and services they offer.[15]

The update to the WhatsApp privacy policy is cosmetic in nature and to a large extent aimed to allow people to communicate with businesses – which businesses are offered through WhatsApp and hosted by Facebook. Also, when messages are conversed with those business accounts, they might be stored and managed by Facebook at the election of the specific business.

Data privacy laws across the world require clear and transparent communications with data subjects. Are we blaming WhatsApp for updating their communication so that users know what is happening in the background? Did you not want to know that?

Therefore leaving aside Signal, is there really such a difference between WhatsApp and Telegram, so much so to necessitate a move from WhatsApp to Telegram? Or do other messaging platforms have a place?

"I think that most people would rather face the light of a real enemy than the darkness of their imagined fears." — **Max Brooks, World War Z: An Oral History of the Zombie War**

[1] Pop-Up notification sent to Android and iOS users.

[2] A Griffen "WhatsApp new privacy terms: What do new rules really mean for you?" available at <https://www.independent.co.uk/life-style/gadgets-and-tech/whatsapp-new-privacy-terms-facebook-rules-explained-b1784469.html>, accessed on 11 January 2021.

[3] A Sha "WhatsApp vs Telegram vs Signal: A Detailed Comparison of Features and Privacy" available at <https://beebom.com/whatsapp-vs-telegram-vs-signal/>, accessed on 11 January 2021.

[4] *Ibid.*

[5] P Karasz "*What Is Telegram, and Why Are Iran and Russia Trying to Ban It?*" available at <https://www.nytimes.com/2018/05/02/world/europe/telegram-iran>, accessed on 11 January 2021.

[6] *Supra* note 3 above.

[7] *Supra* note 3.

[8] *Supra* note 3.

[9] *Supra* note 5.

[10] *Supra* note 5.

[11] *Supra* note 2.

[12] WhatsApp Pay functionality is not as yet active in South Africa.

[13] *Supra* note 2.

[14] WhatsApp privacy policy.

[15] *Ibid.*



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)