An Assembled Critique of WhatsApp's Updated Terms of Use and Privacy Policy

Sanjay Bhattacherjee
Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)
University of Kent

January 14, 2021

Summary

On 4^{th} January, 2021, WhatsApp rolled out updates to their terms of use and privacy policy statements. WhatsApp users have been notified that unless they agreed to the new terms, access to their accounts will be revoked from 8^{th} February, 2021. Although this has not been explicitly mentioned, it is known that inactive accounts (and their data) are deleted after a stipulated period of time.

This document is a summation of my understanding in this context based on the articles I have referred to herein.

To start with, WhatsApp has been sharing user data with Facebook since 2016. Users have been interacting with WhatsApp business accounts that provide customer support and deliver important notifications to their customers. Once these messages are delivered to the business account, they are handled as per the privacy policy of that business. After the current update, businesses can now additionally use the content of the user's messages for "their own marketing purposes, which may include advertising on Facebook". So, based on the messages sent by users to these business accounts, they may see advertisements on their Facebook profile.

End-to-end encryption of messages ensure that WhatsApp servers do not see the content of user messages. However, they collect meta-data like time, frequency and duration of activities on the app, messaging and calling connections, groups, their descriptions, profile photo, device and connection-specific information, location information, et cetera.

WhatsApp Inc. has demonstrated a coercive tendency in its practices. Back in 2016, when they rolled out an update in their terms and privacy policy, the existing users had a choice to opt out of it. New users did not have that choice though. This time, they are enforcing the update on every user - old or new. Even if an individual wants to withdraw themself from the platform, their connections on WhatsApp may not be eager or able to do so. This could be for many reasons - being unable to install or learn to use a new app, limited phone memory that does not allow installation of a new app, most of their contacts are reluctant to shift, or maybe just personal preference.

Users who are not aware of privacy implications of using WhatsApp (or any mobile application for that matter), but are now used to the services will happily "AGREE" to the updated terms and privacy policy. WhatsApp as a company will benefit from this digital (literacy) divide that exists in the society.

This leads us to the next question. The data collected by WhatsApp is used to ensure the quality of performance of the app (as argued in the privacy policy). WhatsApp users use the app to different extent and for different features. Somebody using the app only for messaging a few contacts provides the same data as someone who uses the app extensively with all its features. This is a one-size-fits-all privacy policy and the corresponding application settings provide minimal options to choose what data to share and what not to share. This unilateral policy along with minimalistic choices for data sharing seems inherently unfair. Users should be able to choose the services they want and the chosen services can then inform the user the data they have to provide to WhatsApp to ensure high quality of service.

Finally, Signal and Telegram are two alternatives that WhatsApp users around me are looking at. Signal provides end-to-end encryption of all communication. The client and server application program source code is open for scrutiny by experts. Signal does not store any metadata of a user other than the date of account creation and the date of last use. Hence, Signal does not provide any option for user data backups.

Telegram messages are not end-to-end encrypted by default. However, there is the option to turn on "Secret Chats" that would be end-to-end encrypted. By default, the other messages (called "Cloud Chats") can be backed up and stored on cloud servers managed by Telegram and not any third party. The Telegram mobile application can be verified by a user to be the same as the open source code shared by them.

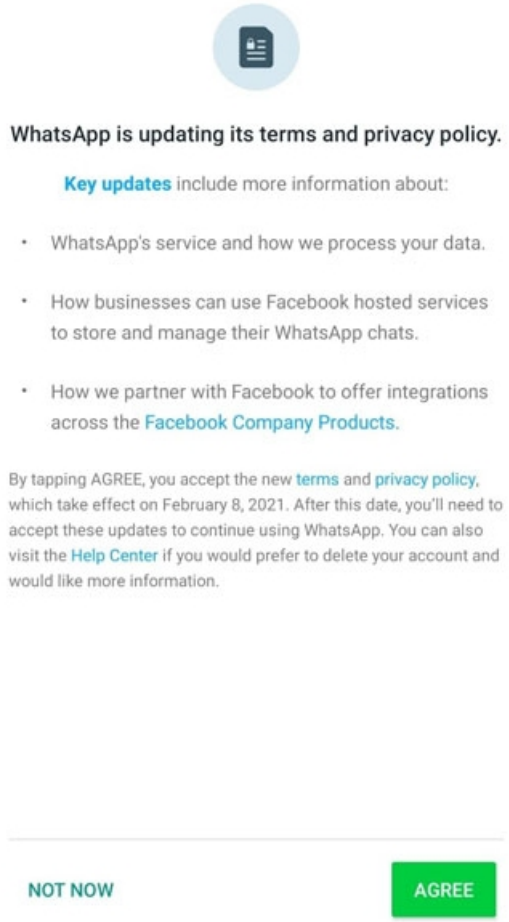

Figure 1: The notification seen by WhatsApp users regarding "Key Updates" in their Privacy Policy, released on 04 january, 2021.

1. **Data sharing with Facebook is not new**
   An old article (dated 13 October, 2016) from the Electronic Frontier Foundation (EFF) stated the following four major security concerns about WhatsApp.
   "Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns"

   (a) Unencrypted backups

   (b) Key exchange notifications

   (c) Insecurity of WhatsApp Web

   (d) Facebook Data Sharing

   This is to point out that WhatsApp has been sharing user data with Facebook, for a long time now. This is made explicit in the privacy policy update of 25 August, 2016 that states:

   > *"We joined the Facebook family of companies in 2014. As part of the Facebook family of companies, WhatsApp receives information from, and shares information with, this family of companies. We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customise, support, and market our Services and their offerings. This includes helping improve infrastructure and delivery systems, understanding how our Services or theirs are used, securing systems, and fighting spam, abuse, or infringement activities. Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads. However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services."*

   It also included the following declaration under "Assignment, Change Of Control, And Transfer".

"All of our rights and obligations under our Privacy Policy are freely assignable by us to any of our affiliates, in connection with a merger, acquisition, restructuring, or sale of assets, or by operation of law or otherwise, and we may transfer your information to any of our affiliates, successor entities, or new owner."

2. **Evolution of WhatsApp's privacy policy**
   As shown in Table 1, there are four WhatsApp privacy policies that are currently available online for the European Economic Area (EEA). The evolution of these privacy policies may be studied for a qualitative and quantitative comparison of information collected by WhatsApp and their implications on user privacy.

EEA	non-EEA
04 January, 2021	04 January, 2021
	20 July, 2020
	19 December, 2019
24 April, 2018	
25 August, 2016	25 August, 2016
07 July, 2012	07 July, 2012

Table 1: WhatsApp's "Privacy Policy" Archive for EEA and non-EEA

3. **Does WhatsApp collect less data from EEA users?**
   In other words, how different are the privacy policies applicable to EEA and non-EEA users? Not much, as far as I have seen in a quick reading. In Table 2 and Table 3, the sections covered in the respective policies are listed for quick comparison. The text is similar for most of these sections. It will require a combination of legal and technical expertise to uncover the "core principles" of the privacy policy that the company abides by unilaterally. On points that they are indeed different, there should be close legal scrutiny.

   For both EEA and non-EEA privacy policy updates on 04 January, 2021, the **Automatically Collected Information** part has three common entries as follows. This shows the wide gamut of information that Whatsapp collects from EEA and non-EEA users alike.

   - Usage And Log Information

     "We collect information about your activity on our Services, like service-related, diagnostic, and performance information. This includes information about your activity (including how you use our Services, your Services settings, how you interact with others using our Services (including when you interact with a business), and the time, frequency, and duration of your activities and interactions), log files, and diagnostic, crash, website, and performance logs and reports. This also includes information about when you registered to use our Services; the features you use like our messaging, calling, Status, groups (including group name, group picture, group description), payments or business features; profile photo; "about" information; whether you are online; when you last used our Services (your "last seen"); and when you last updated your "about" information."

   - Device And Connection Information

     "We collect device and connection-specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, battery level, signal strength, app version, browser information, mobile network, connection information including phone number, mobile operator or ISP, language and time zone, IP address, device operations information, and identifiers (including identifiers unique to Facebook Company Products associated with the same device or account)."

   - Location Information

     "We collect and use precise location information from your device with your permission when you choose to use location-related features, like when you decide to share your location with your contacts or view locations nearby or locations others have shared with you. There are certain settings relating to location-related information which you can find in your device

settings or the in-app settings, such as Location sharing. Even if you do not use our location-related features, we use IP addresses and other information, like phone number area codes, to estimate your general location (e.g., city and country). We also use your location information for diagnostics and troubleshooting purposes."

EEA	non-EEA
https://www.whatsapp.com/legal/updates/privacy-policy-eea	https://www.whatsapp.com/legal/updates/privacy-policy
WhatsApp Legal Info	WhatsApp Legal Info
Information We Collect	Information We Collect
Third Party Information	Third Party Information
How We Use Information	How We Use Information
Information You And We Share	Information You And We Share
How We Work With Other Facebook Companies	How We Work With Other Facebook Companies
Our Legal Basis For Processing Data	-
How We Process Your Information	-
How You Exercise Your Rights	-
-	Assignment, Change Of Control, And Transfer
Managing And Retaining Your Information	Managing And Retaining Your Information
Law, Our Rights, And Protection	Law, Our Rights, And Protection
Our Global Operations	Our Global Operations
Updates To Our Policy	Updates To Our Policy
Contact Use	Contact Use

Table 2: Comparing WhatsApp's "Privacy Policy" Sections for EEA and non-EEA

People around me often ask - what can anybody do with the metadata? Prof. Shujun Li points out that metadata can be quite revealing. As an example, consider two individuals who are regularly messaging each other, until quite late in the night (this can be easily derived based on the location information of the user) and over the weekends. Such information may indicate that they are very likely to be in an intimate relationship. Collating such data about an individual from several platforms can profile that individual by their behaviour and a lot more.

4. **A pattern of coercive practices.**
From the time Facebook took over WhatsApp, the company has been inclined to not give a choice to opt out of its updates. As an instance, we recollect their policy change in 2016. To quote from this EFF article published on 31st August, 2016 on an update released by WhatsApp,

> "From the first time they see the update screen on WhatsApp, existing users have 30 days to click through the privacy policy update, opt out of data sharing, and prevent Facebook from suggesting friends or serving ads based on WhatsApp data. After that, they have an additional 30 days to change their settings further.
>
> As of the announcement of the new policy on August 25, however, new WhatsApp accounts do not have the option to refuse these expanded uses of their data. Instead, the only option available to new users will be whether to join WhatsApp at all under the new privacy policy and all of the data sharing it entails."

Back then in 2016, at least existing users had a choice to opt out of an update. New users did not have that choice. This time they are enforcing the update on every user. The strategy here seems to be to make

EEA	non-EEA
https://www.whatsapp.com/legal/updates/terms-of-service	https://www.whatsapp.com/legal/updates/terms-of-service-eea
About Our Services	About Our Services
Privacy Policy And User Data	Privacy Policy And User Data
Acceptable Use Of Our Services	Acceptable Use Of Our Services
Third-Party Services Licenses	Third-Party Services Licenses
Reporting Third-Party Copyright, Trademark, And Other Intellectual Property Infringement	Reporting Third-Party Copyright, Trademark, And Other Intellectual Property Infringement
Disclaimers And Release	Disclaimers And Release
Limitation Of Liability	Limitation Of Liability
-	Indemnification
Dispute Resolution	Dispute Resolution
Availability And Termination Of Our Services	Availability And Termination Of Our Services
Other	Other
-	Special Arbitration Provision For United States Or Canada Users
Accessing WhatsApp's Terms in Different Languages	Accessing WhatsApp's Terms in Different Languages

Table 3: Comparing WhatsApp's "Terms of Service" Sections for EEA and non-EEA

the users dependant on the "free service" to an extent that withdrawing from it is no more an individual choice. Even if an individual wants to stop using WhatsApp altogether, their contacts on the platform may not be keen to do so. Larger an individual's network, greater is their inertia working against opting out of the platform - even if they are uncomfortable with the update.

We may recollect at this point the tweet from Brian Acton (who co-founded WhatsApp and then the Signal Foundation): "It is time. #deletefacebook". Mass-withdrawal from WhatsApp or Facebook is unlikely. Different individuals would have developed their own level of dependence on the platform that may not be easy to forego. However, it is important for the frog to be wary of the rising temperature of the water around.

5. **One-size-fits-all privacy policy and settings**
The content of our WhatsApp messages is end-to-end encrypted and is hence not visible to WhatsApp. However, they collect all the metadata listed above. If that is put together with the data on Facebook and all other associated platforms owned by the company, it can reveal very intimate details about an individual or as a population as a whole. We have seen instances of such data and analysis being misused.

   The control provided to a user over the metadata collected from them is minimal. Whatever be the extent of use of WhatsApp services (little or large) by an individual, WhatsApp is collecting the same information from everyone.

   The users benefit from the app while the company monetises their data. It is only fair to ask that for every feature or service that the app provides, there should be associated options provided to a user to enable or disable the service and allow for the collection of the corresponding data. Only if a certain service is availed by the user, WhatsApp should collect the data required for it.

6. **Business messaging**
https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en

   > *WhatsApp considers chats with businesses that use the WhatsApp Business app or manage and store customer messages themselves to be end-to-end encrypted.*

   Why does it not know for sure? What part is outside their control? That is answered below.

Once the message is received, it will be subject to the business's own privacy practices. The business may designate a number of employees, or even other vendors, to process and respond to the message.

Some businesses will be able to choose WhatsApp's parent company, Facebook, to securely store messages and respond to customers. While Facebook will not automatically use your messages to inform the ads that you see, businesses will be able to use chats they receive for their own marketing purposes, which may include advertising on Facebook. You can always contact that business to learn more about its privacy practices.

The possible privacy risk of sharing data with business accounts on Facebook may be derived from the above.

7. **Payments on WhatsApp**

   Payments on WhatsApp, which are available in select countries, enable transfers between accounts at financial institutions. Card and bank numbers are stored encrypted and in a highly-secured network. However, because financial institutions can't process transactions without receiving information related to these payments, these payments aren't end-to-end encrypted.

   This feature was launched in India in November 2020 and is currently available to 200 million users (out of the total of 400 million WhatsApp users). To quote from this 6^{th} November, 2020 article:

   > "Starting today, people across India will be able to send money through WhatsApp. This secure payments experience makes transferring money just as easy as sending a message," WhatsApp said in a blog post.

   This required WhatsApp to store its data locally in India as mentioned in this article.

8. **The Facebook Companies**
   WhatsApp policies say that they may share data with other Facebook companies

   > "In addition to the services offered by Facebook Inc. and Facebook Ireland Ltd, Facebook owns and operates each of the companies listed below, in accordance with their respective terms of service and privacy policies. We may share information about you within our family of companies to facilitate, support and integrate their activities and improve our services. For more information on the Facebook Companies' privacy practices and how they treat individuals' information, please visit the following links:
   >
   > - Facebook Payments Inc. (`https://www.facebook.com/payments_terms/privacy`) and Facebook Payments International Limited (`https://www.facebook.com/payments_terms/EU_privacy`)
   > - Onavo (`http://www.onavo.com/privacy_policy`)
   > - Facebook Technologies, LLC and Facebook Technologies Ireland Limited (`https://www.oculus.com/store-dp/`)
   > - WhatsApp Inc. and WhatsApp Ireland Limited (`http://www.whatsapp.com/legal/#Privacy`)
   > - CrowdTangle (`https://www.crowdtangle.com/privacy`)"

9. **Switching to other services**

   (a) Signal is maintained by a United States 501c3 nonprofit - Signal Foundation. Signal stores minimal metadata about its users. It uses end-to-end encryption and the server as well as the mobile app client code is open-source. Regarding the metadata collected by Signal and their data sharing practices, this blog post is reassuring.

   > *"We've gotten a lot of questions at Signal... so we wanted to briefly recap how it is that we've designed Signal, and how we think about concepts like privacy, security, and trust...What if the worst should happen, and some unauthorized party were to compromise Signal? We don't have to speak hypothetically, because the US government already tried this... In 2016, the US government obtained access to Signal user data through a grand jury subpoena from the Eastern District of Virginia. However, there wasn't (and still isn't) really anything to obtain. At the time, we worked with the ACLU to fight the gag order that was intended to prevent us from publishing this information, so you can see the full subpoena and response here. The only Signal user data we have, and the only data the US government obtained as a result, was the date of account creation and the date of last use – not user messages, groups, contacts,*

profile information, or anything else. This is because we've designed Signal to keep your data in your hands rather than ours. Signal uses end-to-end encryption so that we never have access to the contents of the messages you send; they are only visible to you and the intended recipients. However, Signal also applies this design philosophy to the rest of your data as well... We also make this technology publicly available for free because Signal is a 501(c)(3) nonprofit. Our mission is to increase privacy online, so we publish our technology and share knowledge to encourage other companies to adopt it in their own products and services."

The terms and privacy policy of Signal are in alignment with the above.

(b) Telegram (`https://telegram.org/faq#q-so-how-do-you-encrypt-data`) messages are encrypted only for "Secret Chats", and not otherwise. Its source code, protocol and API are open. However, normal messages get decrypted at the servers. They justify the choice of not using default end-to-end encryption primarily for backup of user's message history in the article "Why Isn't Telegram End-to-End Encrypted by Default?"

Interestingly, they provide a tool for users to check that the app's source code published by them is indeed the version that is installed on Android or iOS phones. This verifiability is reassuring and should be adopted by other apps as well.

They have also critiqued the end-to-end encryption of Whatsapp in the article titled Why the WhatsApp backdoor is bad news.

Acknowledgement. I would like to thank Shujun Li, Mahaprajna Nayak and Jason Nurse for helpful discussions.