How do Whatsapp, Telegram and Signal Share Data with Third Parties?

After a massive outrage from the general public and the platform's users, against Whatsapp's new updated policy, the popular messaging platform decided to delay their decision to implement the new policies. A lot of this outrage was also caused due to some misconceptions which were appealing to a larger audience and brought in a greater audience towards the people who were spreading these misconceptions and misinformation (which ultimately was turning out to be beneficial for them). A lot of these claims made by these people highlighted certain aspects (about data collection and data sharing) in the policy which, according to them, were newly added, but in reality, these aspects were already present and rather just extended and explained further, except a few aspects which were only added due to the recent developments and allowances provided by the Indian Authorities and regulators to the platform. This particular blog takes one through those aspects of data collection and will explain exactly how Whatsapp shares the collected data with third parties, including law enforcement agencies. The blog will also try to draw a parallel with other similar platforms(signal and telegram) in this regard.

What data does Whatsapp, presently, collect ?

If anyone carefully reads the existing privacy policy of Whatsapp, they will realize that they have already agreed to such terms which allow for all kinds of data being collected. This includes:
Expressly provided Data :

This category contains all kinds of Data which an Individual expressly provides the platform to use its services. It includes :

1. **(A.) Account information :** the following data can be considered as your account information.

- Mobile number
- Profile Picture
- Status Message
- Profile Name

(B.) Encrypted information : The other information kinds of information which one provides and is subsequently collected by the platform is either stored in an encrypted format or not stored at all, as is transmitted while being End to End encrypted. This includes messages, location, voice recordings, media files, documents, calls, video calls, payment data, location. However, the situation becomes slightly different when one shares this data with a third party. It will be explained later in the blog.

2. Automatically collected Data

A lot of information is automatically collected and stored by WhatsApp, with regards to one's usage of the platform. This includes :

- Usage and Log Information : this includes activity on the platform, log files, performance logs and reports.
- Device and Connection Information : this includes hardware model, operating system information, browser information, IP address, mobile network information including phone number, device identifiers and location information as well(when one shares their location with other individuals).
- Cookies : the activity on WhatsApp web or accessing WhatsApp's online resources like FAQ's etc are collected as cookies.
- Status Information : the last seen and whether an individual is online or not is also collected.

Sharing of data

A lot of these aforementioned types of data are also being shared with the other parties as well, for several reasons.

Data Shared with Facebook : All the above-mentioned categories of data is shared with Facebook which includes account registration information, transaction data, service-related information, information on how one interacts with others (including businesses) when using WhatsApp, mobile device information, IP address. Whatsapp claims that they use this data "to help operate, provide, improve, understand, customize, support, and market our Services and their offerings." The above-used language already has a very wide ambit and further even includes that Facebook, Whatsapp and other sister companies (subsidiaries of Facebook or Facebook companies) can also use this data for "making product suggestions (for example, of friends or connections, or interesting content) and showing relevant offers and ads "making product suggestions and showing relevant offers and ads." It becomes very obvious that Facebook already collects and uses information from WhatsApp to sell products on its platform by profiling the individual from their device hardware information, network information, account information, activity etc.

Data Shared with Third Parties: The situation where data is being shared with third parties is quite peculiar as the platform does not clearly explain which entities exactly are the 'third parties'. The platform in their policy just highlights the working through an example where they explain that if a 'third-party service', like Google drive, which is built with their platform, is receiving the data then their own privacy policy, i.e. third party service's privacy policy, will apply as the data is directly being shared with them. One should realize that this data could also be the messages an individual sends, as one can have a backup of their messages in Google drive. However, presently one can argue that businesses which use WhatsApp business accounts have their services built with

the platform, and multiple people in a business can receive and access that data which one shares with the business, including the conversation they are having using the platform. While the messages and conversation remain End to End encrypted, multiple people can access those messages. This essentially means that the update mentioned in the new policy which talks about "One's interaction with business account" can already be covered under this clause.

Data sharing with Law enforcement

Whatsapp's entire infrastructure and management is located in the United States and this fact affects the law enforcement agencies of a lot of countries, especially the one's which don't have a strong data protection law. The law enforcement agencies of the United States have it is a lot easier to get the following information from WhatsApp :

- Basic subscriber information like name, service start date, last seen date, IP address and email address) by providing the platform with a valid subpoena.
- Other information about the account, not including contents of communications, which may include numbers blocking or blocked by the user, in addition to the basic subscriber records identified above through a court order issued under 18 U.S.C. Section 2703(d) or
- Stored contents of any account, which may include "about" information, profile photos, group information and address book, if available, provided they get a proper search warrant, as described in their federal criminal procedure and showing a probable cause.

However, for the law enforcement agencies located outside the jurisdiction of the United States, it is very difficult to get any type of data from Whatsapp. The biggest and the most fundamental reason behind the same is the time-consuming process of acquiring the data through diplomatic channels. This includes sending data requests or court orders via Ministry of external affairs through the process and method described in the Mutual Legal Assistance treaty or through the letter rogatory. While WhatsApp does state that it assists the law enforcement agencies by assessing the requests through international standards taking into account human rights, due process, and the rule of law. However, as far as India Is Concerned, in the best-case scenario, one can't expect more assistance than receiving Basic Subscriber information after sending a notice u/s 91 CRPC, if one wishes to not go through the proper diplomatic channels.

Trends with Signal

One of the key features of the platform, which is appealing to a lot of people, is that the platform does not collect any information relating to the individual's interaction with the platform except the mobile number, which is required for account registration. Even the addition of profile picture and profile name, which is voluntary, is encrypted.

Third-party interaction

The platform does work with third parties to provide their services but in these cases, the privacy policies of those platforms would apply.

Interaction with Law enforcement

While the platform does share the information they hold against a valid subpoena and valid request from Law enforcement agencies, but there is not much information to share in the first place. In a blogpost, the platform highlighted that In 2016, the US government obtained access to Signal user data through a grand jury subpoena from the Eastern District of Virginia. This subpoena, however, only provided the government with the date of creation of an account and the last date of connection of the account with the Signal server.

Telegram

The platform also has a similar vision to Signal or the Open Whisper Sytems. The platform doesn't even require an individual's phone number to register, one can register with the platform just by their username, which doesn't need to be their real name. All further information including profile name, profile picture and about information is voluntary. Other than the email address, which one can provide with as a recovery email id for 2 step verification or password recover, or cookies, for enhancing web experience, and the above-mentioned information, the platform does not collect any information or uses it for any marketing purposes.

Third-party interaction

The information is not shared with any third party in any case. The payment data is directly provided to the transaction agent or payment provider and is stored with them and not with the platform. One can also delete the entered payment and shipping information which are with these providers by going to Telegram Settings > Privacy & Security > Data Settings and selecting 'Clear Payment & Shipping Info'.

Interaction with Law Enforcement

While the telegram's public channel features allow for the authorities to remove the content but as far as other features are concerned the platform does not share any information with any law enforcement agency as the data stored is located at multiple locations, which would require one to get access to diplomatic channels of all those locations, which is virtually impossible. However, the platform will share the phone number and IP address of a user if they receive a valid cord order which confirms that the user is a terrorist.