

# Data & Information Management

## 1. PickMe

PickMe is a platform that is providing services in Sri Lanka such as ride taking, package delivering and food delivery. To accomplish these services pickme depend on data such as user location, destination to travel, driver location and other payment details.

When I use pickme for my transport and to get my food from restaurants from which I like, the app uses my Realtime data most importantly my current location (live location), contact number and also the destination to check for a driver nearby to match with me for my ride. Also, when delivering stage, they also collect information's like my address, restaurant address and driver location to complete the ride efficiently and effectively. Once we book a ride we will get information of the driver such as, vehicle no., contact number and location if we didn't get those it would be hard to contact the driver to direct him to us and it would be hard to identify who is the driver.

The data is been generated by the user when he/she interact with the app and get a driver through the app. When user book a ride the booking information and the location history is been stored as rider data. These information's been stored in the pickme's servers while the technical professionals working the backend to connect customers with drivers.

Pickme collects information's such as location, contacts, transaction, usage and preference, calls and SMS, device and log.

- Location information: if the location falls into wrong hands, they can also track and monitor individuals this can cause physical safety risk.
- Contact information: if the personal contact number is got leaked it can cause that individual might face phishing attacks and identify theft lead to privacy breaches.
- Transection information: leaking of transection information like card details and banking information's can cause financial fraud and unauthorized purchases. It also can harm individual reputation since those are confidential and sensitive.
- Calls and SMS information: leakage of calls and SMS can expose each personal sensitive conversation, contacts and communication details. And also, it can be used to for blackmailing an individual which also a mean of privacy breach.

To safeguard all the security measures pickme has to give priority to their data security, conduct bug bounty programs to patch up vulnerabilities and maintain transparency in their practices.

## 2. WhatsApp

WhatsApp is one of the world's popular application that allows user to share messages, videos, images, voice messages, video calls and more. WhatsApp provides fast and simple service at no cost. WhatsApp also collects a bunch of data from the user such as personal information, contacts, messages, media files, location data and more and stores it. Using of contacts to identify and message the other WhatsApp user.

I am using WhatsApp daily to communicate and interact with my friends and family. WhatsApp depend on my contacts, messaging and media files to provide a reliable and effective experience through out using the app. The storage media of WhatsApp allow me to share images, videos and documents with relevant people. Without access to the above needed data WhatsApp will not be able to identify and enable the ability to communicate with others. The main functionality of the application would be badly get damaged and go unfunctional.

WhatsApp data is been generated by the user when he/she is interacting with the application through calls or messages. All the messages, calls, shared documents or media files are being stored in the WhatsApp servers for a shorter period and then get deleted. Some of the data may be stored permanently to improve and upgrade their service. WhatsApp states that they do not retain users' messages on their servers. Moreover, the encryption process and the data transections are been monitors and managed by the WhatsApp engineering and technical teams. WhatsApp implements end-to-end encryption which allows only the sender and the receiver can access the content of the message.

Even WhatsApp addresses that the messages are end-to-end encrypted still WhatsApp had mentioned in their official site that they also share information's like account registration information, transection data, service-related information, device information, IP address, location and more with their meta companies.

- Even though the content of the message is been encrypted metadata like contact information and call and message duration may still be obtained.
- WhatsApp also share some user data with their meta companies like Facebook for advertainment purpose and other, this rise the concern on the data privacy and usage more.
- By providing third-party access there is a high risk of unauthorized access to user account by malicious attackers.

WhatsApp must definitely give much priority on their data security and management by considering the user privacy and identity. WhatsApp also provide backup facility to the cloud, this also could bring high risk if it is not been monitored and managed properly.

### **3. Google**

Google is a technology company which provides more than 50 internet services including search engine, cloud storage, email services, tools for productivity, software's and more. It is also a multinational company. Google also collect information from the user to process and upgrade their services, this include usage data & preferences, Gmail messages, G+ profile, photos, videos, browsing history, map searches, docs and more. Google also collect and analyses the search queries entered by the user, location data to improve the search result in that location, collects usage data to keep track of user interaction with their services.

In my daily routine bases I use google services a lot for searching for information for my assignments, emailing, accessing google classroom and more. I get through various of sources through the google search and gain much comfort with the cloud and email services which makes an effective and efficient usages for all the students as me. If google data was not available, I would through back to a huge way back in technology where I would miss a huge amount of information. Even if I had used any other alternative it would be not much effective and user-friendly as google.

Data is generated for google through user interaction towards their services like making search quires, accessing Gmail and using google map to identify location and more. These data are captured and sent to the googles servers for processing. Here the data is been analyzed, stored and security measures are been implemented.

As in all the applications google also has several risks related to privacy and security on user data. Google collects data from user and create individual profiles for each which also can be a threat to the user if the credentials are been stolen or leaked. Google also share user data with third-party companies for advertisement or for static purposes which also will effect the user privacy.

It is a mandatory thing for each user who uses google services to be concern and aware of the privacy policies and settings which are been displayed. It is a must for everyone to consider on how their data is been collected, shared and used among these services.

## Reference

1. USER PRIVACY STATEMENT. (2016). Available at: <https://pickme.lk/themes/pickme/assets/pdf/pickme-privacy-policy.pdf> [Accessed 3 Aug. 2023].
2. The PickMe Engineering Blog. (2021). The PickMe Engineering Blog. [online] Available at: <https://blog.pickme.lk> [Accessed 3 Aug. 2023].
3. www.dpconline.org. (n.d.). A Case Study – WhatsApp Records Capture - Digital Preservation Coalition. [online] Available at: <https://www.dpconline.org/blog/wdpd/whatsapp-records-capture> [Accessed 3 Aug. 2023].
4. faq.whatsapp.com. (n.d.). WhatsApp Help Center. [online] Available at: [https://faq.whatsapp.com/?locale=en\\_US](https://faq.whatsapp.com/?locale=en_US) [Accessed 3 Aug. 2023].
5. policies.google.com. (n.d.). ‘collect information’ – Privacy & Terms – Google. [online] Available at: <https://policies.google.com/privacy/example/collect-information?hl=en>.
6. Google.com. (2000). Privacy Policy – Privacy & Terms – Google. [online] Available at: <https://policies.google.com/privacy?hl=en>.
7. What Does Google Do With Your Data? (n.d.). What Does Google Do With Your Data? [online] Available at: <https://www.avast.com/c-how-google-uses-your-data>.
8. www.youtube.com. (n.d.). Complete data lifecycle on google cloud using 21 gcp products - under 10 mins. [online] Available at: <https://www.youtube.com/watch?v=8p-qLtqlJpQ&t=324s> [Accessed 4 Aug. 2023].