TRADING PRIVACY FOR A CHEAP TRANSPORT SYSTEM

UPDATE: 10th November, 2020.

As a result of our technical research and advocacy on Safeboda, the company made changes in relation to its data protection principles by prompting users to review the privacy policy, terms and use before using their services. The company also proceeded to publish a link to its privacy policy on the official website. However, key concerns remain; the company's android application still contains third-party trackers like ***CleverTap.***

INTRODUCTION.

With the introduction of apps and services where business models rely on the collection, processing and sharing of personal information, people wonder how they can still have control of their information in this digital context. It is thus important to know, among others, what happens to our data once it is collected, how we can access, correct or delete it, how long it will be retained and whether it is shared with any third parties.

Companies have obligations when it comes to their data practices so as to prevent any risk of data exploitation and surveillance, and they must also have privacy policies in place so as to meet their informational and transparency requirements.

It is a legal requirement for companies to inform individuals who use their products and services about how their data is being processed[1]. This is the purpose which a Privacy Policy, a legal document that guides the collection, processing, and use of the personal data serves. It should be in a comprehensive and clear language that can be easily understood by any person[2].

Any company's processing activities contained in their Privacy Policy must comply with Uganda's Data Protection and Privacy Act, 2019[3]

In 2019, we carried out an evidence-based research about the Safeboda privacy policy and its practice, considering that it is Uganda's leading transport application.

When reviewing the privacy policy and comparing it to how the app operates in practice, we identified a number of discrepancies. Over the course of our research, Safeboda updated its Privacy Policy on the 4th November 2019.

What is SafeBoda?

Safeboda is a community of entrepreneurs and Boda drivers working together to improve professional standards across the urban transportation industry in Africa[4]. Their stated social mission is to improve the welfare and livelihoods in Africa by empowering people. Ricky Thomson, Alastair Sussock, and Maxime Dieudonne are the co-founders of Safeboda. It reports to have coverage in countries like Kenya, Uganda, and Nigeria[5].

Like most apps, Safeboda's processes users' information to provide its services. This app works by the user opening the Safeboda app on their mobile device, typing in the destination then requesting for a rider, who picks the user from their location and payments will be done once

[1] Section 7 of the Data Protection and Privacy Act 2019

[2] Similar obligations are imposed by other data protection laws. See, for example, EU General Data Protection Regulation, Recital 61 and Article 12.

[3] https://www.unwantedwitness.org/download/uploads/THE-DATA-PROTECTION-AND-PRIVACY-ACT-2019-min.pdf

[4] Safeboda.com/ug/index.php/about-us

[5] https://digestafrica.com/safeboda-barcelona-daily-brief

the user reaches the destination [6]. There are over 1,000,000[7] people using the Safeboda app in Uganda. Safeboda has over 6000 riders in its networks within Uganda's capital Kampala.

In 2019, we carried out evidence-based research about the SafeBoda privacy policy and practice. Our finding showed that the Safeboda privacy policy was not clear and some of its provisions did not seem to be entirely in line with the Data Protection Act 2019 and internationally recognized data protection standards.

Comparison between the previous SafeBoda privacy policy and the current SafeBoda privacy policy that was updated in 2020.

The data protection principles of fairness, lawfulness, and transparency require the data controller to inform users about the sharing of personal data with third parties. Data subjects have a right to limit or stop the processing of personal data in particular circumstances. This leaves the data controller with the onus to provide evidence that such sharing of data with third parties is necessary to provide the service as a data controller shall only process the necessary personal data required for a specific purpose[8].

This was addressed under Clause 12.1.2 of the new SafeBoda privacy policy that[9]:

> *if the personal data is used to communicate with the data subject, when the first communication is made; or if the personal data is to be transferred to another party, before that transfer is made; or as soon as reasonably possible and in any event, not more than one month after the personal data is obtained then the data subject will be informed of its purpose*.

[6] https://safeboda.com>indexphp>faqs
[7] From google play store as of 23 June 2020
[8] Section 14 of the Data Protection and Privacy Act
[9] http://safeboda.com/policy/privacy/

An extract from the old privacy policy.

What personal information do we collect from the people that visit our blog, website or app?

Customer contact information

When ordering or registering with our app, as appropriate, you may be asked to enter your name, email address, phone number, credit card information or other details to help you with your experience.

With your consent, we also receive basic contact information (name, email, phone number) from Google and Facebook when you register with the SafeBoda app. This information is used to identify customers, manage their account, and continuously improve the customer experience.

When we analyzed the above extract[10] from the older Safeboda privacy policy[11], the phrase "or other details" did not provide sufficient information to the user, about what data was being collected directly and what data was processed as part of the app usage. To comply with transparency obligations imposed by data protection and privacy legislation, Safeboda as a data collector should have stated all the categories of personal data as well as personal data that was collected from the users directly or indirectly from other sources in an exhaustive manner. Failing to do so raised questions regarding the compliance of the privacy policy with the principle of transparency and hindered the ability to uphold the right of users to be informed about the data collected from and about them[12].

Sharing personal data with third parties

The older privacy policy referred to third party data sharing/disclosure as follows:.

Third-party disclosure

We do not sell, trade, or otherwise transfer to outside parties your Personally Identifiable Information unless we provide users with advance notice. This does not include website hosting partners and other parties who assist us in operating our website, conducting our business, or serving our users, so long as those parties agree to keep this information confidential. We may also release information when it's release is appropriate to comply with the law, enforce our site policies, or protect ours or others' rights, property or safety.

However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

[10] Screenshot was taken on 5th October 2019
[11] www.safeboda.com privacy policy was last edited on 2017/02/22
[12] Section 3(1)(f) Data Protection and Privacy Act,2019

Caption: Extract[13] from the previous Safeboda privacy policy.

According to this clause, data was disclosed to third parties, only with users' "advance notice" and not consent, which would be the required legal basis to disclose personal data to third parties. In other words, the older Safeboda privacy policy suggested that as long as users knew that their personal data was to be transferred to third parties, this should be enough to render the transfer compliant with data protection laws without the user actually consenting to such transfers.

The new privacy policy shows that the data subject "will be informed before " the data is shared with the third party under clause 12.1.2; however, this is still not consent because the moment the subject data objects to the collection or processing of personal data, the person who's collecting or processing personal data shall stop the collection or processing of personal data[14]

In their old privacy policy, user data could be shared for third-party behavioral tracking in absence of consent from the user. So this amounted to transfer of data to third parties without consent which might not only potentially be a breach of the obligations of the data controller but also a breach of trust between users and the data controller.

As per the data protection principles[15], the data subject needs to know in advance what data is being processed as well as what data is being shared and who are the recipients of that data so as to make an informed decision to consent to the sharing of their data. Consent is a core principle of data protection which allows the data subject to be in control of when and how their personal data is being processed and it should be freely given, specific, informed, and unambiguous this can be in a written form or oral[16].

Data Retention

Whereas storage limitation is a key data protection principle, the previous SafeBoda privacy policy did not provide any information about the exact retention periods of personal data. It is nevertheless necessary that a data controller shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data is collected and processed. As provided for in Section 18 of the Data Protection and Privacy Act, the data controller should specify the retention period for which the data will be kept[17].

An entity collecting personal data shall inform the data subject about the period for which the data will be retained to achieve the purpose for which it is retained[18].

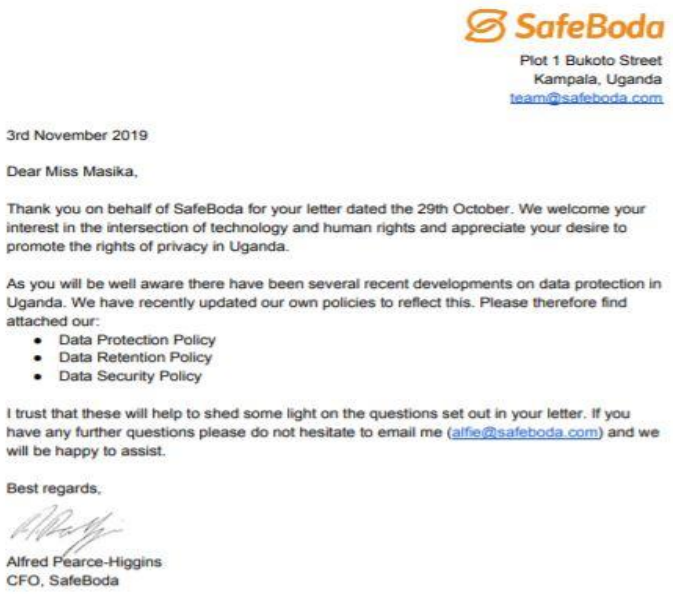
---

[13] Captured on 5th October 2019
[14] Section 7 (3) of the Data Protection and Privacy Act
[15] Section 3 (1) (f) of the Data Protection and Privacy Act 2019
[16] Section 7 of the Data Protection and Privacy Act 2019
[17] Section 18(1) Data Protection And Privacy Act 2019
[18] Section 13(1) (I), Data Protection And Privacy Act 2019,

Clause 7 of the new SafeBoda privacy policy[19] states that, as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed. However, the privacy policy does not specify the exact retention periods for every category of personal data of users. This raises some important transparency questions and might potentially hinder users' ability to properly be in control of their personal data by knowing for how long each data will be kept and under what legal basis.

In November 2019, we sent SafeBoda Company an email seeking their clarity on certain issues we had raised in the email after realizing that the previous SafeBoda privacy policy seemed to not be in line with the Data Protection and Privacy Act 2019.

This was the reply from SafeBoda:



SafeBoda

Plot 1 Bukoto Street
Kampala, Uganda
team@safeboda.com

3rd November 2019

Dear Miss Masika,

Thank you on behalf of SafeBoda for your letter dated the 29th October. We welcome your interest in the intersection of technology and human rights and appreciate your desire to promote the rights of privacy in Uganda.

As you will be well aware there have been several recent developments on data protection in Uganda. We have recently updated our own policies to reflect this. Please therefore find attached our:

- Data Protection Policy
- Data Retention Policy
- Data Security Policy

I trust that these will help to shed some light on the questions set out in your letter. If you have any further questions please do not hesitate to email me (alfie@safeboda.com) and we will be happy to assist.

Best regards,

Alfred Pearce-Higgins
CFO, SafeBoda

Our engagement with Safeboda over potential shortcomings of their data processing activities and the lack of clarity of their privacy policy seems to have also prompted them to upload a new privacy policy[20] on their website putting into consideration the Data Protection and Privacy Act, 2019 and the data protection principles.

POLICY AGAINST PRACTICE

Between October 2019 and March 2020, Unwanted Witness carried out a technological analysis on the Safeboda app using the following components:

- A laptop running a virtual machine (using Oracle's VirtualBox) with mitmproxy in "transparent" mode (this implies that the connection is intercepted without the knowledge of the client). Along with the necessary tools to create a functional network

[19] http://safeboda.com/policy/privacy/
[20] The new privacy policy was uploaded on 4th November 2019

access point. The virtual machine runs Debian 10 operating system due to the requirements of mitmproxy using python 3.6.4 or later.

- An Android phone running Android 8.1 (Oreo). We used another android phone running Android 6.0 in the latter test.
- A device (laptop) to run the Android Development Bridge (ADB) in order to install the mitmproxy certificate into the Systems Trust Store (as opposed to the Users Trust Store) due to security constraints introduced in Android 7.

On transit, data is encrypted using Transport Layer Security between the third-parties like Facebook and the Safeboda App. By using the free and open-source tool called mitmproxy, we were able to decrypt and encrypt data that's in transit between third-party's servers and our android phone (this process is also referred to as "man-in-the-middle"). Mitmproxy decrypts and encrypts data packets on the fly by camouflaging as a remote secure point. We also added the mitmproxy's public key to our android phone as a trusted authority. The data stays on our phone during the decryption process.

The following steps were taken when testing the Safeboda application:

- Connect to a non-intercepting Wi-Fi
- Download the Safeboda application from the Google Play Store.
- Connect to mitmproxy Virtual Machine via Wi-Fi.
- Open the Safeboda app and interact with it for 5 minutes (this included activities like; requesting for a motorcycle rider, submitting ~~in~~ destination et cetera.)

Observations.

a. **Initial Analysis**

   In October 2019, we discovered that the Safeboda app was sharing data with Facebook without the consent of the users. The app used a Facebook business tool known as Software Development Kit (SDK). Through this SDK, Facebook routinely collected information on Safeboda's users via the Safeboda app. The SDK is a set of development tools that helps developers to build apps for a specific operating system; it allows developers to integrate their apps with Facebook's platform and contains a number of other components such as analytics, Ads, Log in, Account Kit, Share, Graph API, App Events and App Links.

   The SDK collected information on Safeboda users and sent it to Facebook ~~servers~~, regardless of whether they were Facebook users or not; this meant that even if the user didn't have the Facebook app installed on their phone or a Facebook account, the Safeboda app would still send data to Facebook.

The screenshot[21] below shows an event's data that was taken from the Privacy International's [data interception environment](#) [22] from which we used mitmproxy to intercept communications between a phone and Facebooks servers;

The second last field from the above screenshot (extinfo:) clearly shows that the application sends user's data such as the screen size ("1080, 1794"), android version ("8.1.0"), location basing on the time zone ("Africa/Nairobi[23]"), telecommunications provider ("Safaricom") and other information to Facebook. In addition, the Advertising ID (advertising_id) is also transmitted, which can uniquely identify an individual device.

The following response is generated after the above request, indicating successful capture of this information by Facebook;

b. Recent Analysis

Following a letter we sent to the company asking for clarifications, the company removed Facebook trackers from its application. Although Safeboda removed Facebook trackers, it added two new trackers that is to say; CleverTap and Amplitude.

This means that every time a user uses the Safeboda app, it still sends users' data to third-parties like CleverTap without user consent as soon as the app is launched.

[21] Taken on 2nd October 2019
[22] https://privacyinternational.org/mitmproxy19
[23] The test was carried out in Nairobi, Kenya.

CleverTap which is formerly known as WizRocket is a SaaS-based customer lifecycle management and mobile marketing company headquartered in Mountain View, California[24]. Founded in May 2013, it provides mobile app analytics[25].

The company brands itself as a company that helps other companies to build valuable, long-term relationships with their customers by giving them two things: access to real-time behavioral analytics so they know who they are, and a platform with which they can engage users on the right channels, at the right time, and with a message that resonates[26]

It is not the first time CleverTap is involved in cases of sharing users' data without their consent. Privacy International discovered this tracker before in menstruation applications[27]. The users' data that's shared include; the phone type that the user is using, phone contact, email address, location, time-zone, user-names, email address and their carrier (Internet Service Provider).

The screenshots[28] below shows some of the data that the tracker transmits without the Safeboda users' consent. It was taken from Privacy International's data interception environment.

[24] https://clevertap.com/contact-us/
[25] https://clevertap.com/about-us/
[26] Extracted from CleverTap's official website
[27] https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data
[28] The screenshots were taken on 20th March, 2020

Request | Response | Details

POST https://wzrkt.com/a1?os=Android&t=30603&z=R5K-R7Z-975Z&ts=1584700926 HTTP/1.1

Content-Type	application/json; charset=utf-8
X-CleverTap-Account-ID	R5K-R7Z-975Z
X-CleverTap-Token	1a2-352
User-Agent	Dalvik/2.1.0 (Linux; U; Android 6.0; Infinix HOT 4 Lite Build/MRA58K)
Host	wzrkt.com
Connection	Keep-Alive
Accept-Encoding	identity
Content-Length	1615


```
[
    {
        "af": {
            "Build": "3003011",
            "Carrier": "Airtel UG",
            "Make": "Infinix",
            "Model": " HOT 4 Lite",
            "OS": "Android",
            "OS Version": "6.0",
            "SDK Version": 30603,
            "Version": "3.3.11",
            "cc": "ug",
            "dpi": 320,
            "hgt": 4,
            "useIP": false,
            "wdt": 2.25
        },
        "ait": 0,
        "arp": {
            "av": "3.3.11",
            "d_ts": 1584696716,
```


The tracker extracts both of the user's current and final destinations and send them to wrkt.com


```
{
    "dsync": false,
    "ep": 1584700925,
    "evtData": {
        "default_payment_method": "CREDIT",
        "from_address": "792 Sentema Rd, Kampala, Uganda",
        "from_latitude": 0.3181788,
        "from_longitude": 32.5491234,
        "price": 2000,
        "to_address": "Wandegeya, Wandegeya, Kampala, Uganda",
        "to_latitude": 0.3337535,
        "to_longitude": 32.5683826
    },
    "evtName": "ride_estimation",
    "f": false,
    "lsl": 0,
    "pg": 1,
    "s": 1584700875,
    "type": "event",
    "wzrk_error": {
        "c": 512,
        "d": "For event \"ride_estimation\": Property value for property promo wasn't a primitive (null)"
    }
},
{
    "dsync": false,
    "ep": 1584700925,
    "evtData": {
        "from_address": "792 Sentema Rd, Kampala, Uganda",
        "from_latitude": 0.3181788,
        "from_longitude": 32.5491234
    },
    "evtName": "ride_select_origin_location",
```

Safeboda Response on CleverTap Trackers

Before this report was published, we submitted our findings to Safeboda and this was the response from the Chief Financial Officer on the use of CleverTap:

> "I have spoken to the tech team about our use of Clevertap. Clevertap is an analytics tool that is use for tracking marketing communication and identifying product issues. It does not have the right to use that data for any purposes and as such is akin to storage of data on AWS or any other storage/analytics tool. If you believe that it would be appropriate then we can amend our Customer Terms of Use that some data is stored on servers operated by third party data processors. The Data policies already make reference to 'third-party data processors'."

From the above response, Safeboda doesn't deny the fact that it uses CleverTap Tracker in its application and the Privacy Policy does indicate that third parties may be given access to the data for analytics purposes. However, processing for marketing and analytics purposes is a different purpose than providing the service. This means that data controllers shouldn't bundle consent altogether for all purposes but ask users to provide consent in a granular way. This way users get to know what they are consenting to and they are equally offered a choice to say no to processing operations that are not strictly necessary for the provision of the services. The application should provide the user with a choice to opt out from their data being shared for marketing and analytics purposes.

Recommendations

Although Safeboda made some improvements such as updating its privacy policy and removing Facebook trackers from its application, it might still have to make more adjustments to meet the required data protection standards and principles:

1. Safeboda should offer users a genuine choice to consent to the processing of their data for marketing and analytics purposes, including via third parties like CleverTap that may act as processors. Bundling consent negates users' choice.
2. The privacy policy should show the date it was last modified to allow individuals to track any changes made by the company.
3. The company should exhaustively specify the third-parties and the exact personal data it shares with them in its privacy policy.

Conclusion

We urge companies, institutions, and government agencies to adhere to the existing legal frameworks without the government's or civil society's intervention. We call upon other companies to prioritize users' data and desist from using technology that exploits it. Unwanted Witness will keep on exposing companies, institutions, and agencies that engage in data exploitation practices, and we will continue advocating for change.