

**NATIONAL INFORMATION TECHNOLOGY
AUTHORITY, UGANDA
(NITA – U)**

**Investigation report into allegations of unlawful
sharing of SafeBoda users’ personal data without
their consent by Guinness Transporters Limited
*trading as SafeBoda***



1. INTRODUCTION

1.1 Background

The Ministry of ICT and National Guidance submitted to the National Information Technology Authority, Uganda (NITA-U) a petition/complaint received from the office of the Speaker of Parliament of Uganda, made by Mr. Obedgiu Sammy. Mr. Obedgiu alleged that Guinness Transporters Limited *trading as* SafeBoda was implicated in an investigation report by a Civil Society Organisation – Unwanted Witness, for sharing its users’ personal data without their consent. A copy of the petition and the Unwanted Witness report are attached hereto and marked Annex “A” and Annex “B” respectively.

Upon receipt of the complaint, NITA-U commenced investigations in accordance with Section 32 of the Data Protection and Privacy Act, 2019 and this report provides findings and recommendations of the investigation.

1.2 Brief on SafeBoda

SafeBoda is a platform operated by Guinness Transporters in Uganda and SafeBoda Nigeria in Nigeria¹. SafeBoda connects motorcycle taxi riders with passengers/users by collecting users’ personal data through the application. This application works by the user opening the SafeBoda application on their mobile device, typing in the destination then requesting for a rider, who picks the user from their location and payment will be done once the user reaches the destination².

2. REVIEW SCOPE AND OBJECTIVES

2.1 Purpose and scope of the investigation

As the regulator for data protection, NITA-U is required to investigate complaints made against a data collector, data processor or data controller to

¹ SafeBoda ‘2019 Data Protection Policy’ and SafeBoda ‘Employee Handbook’.

² <https://safeboda.com/ug/index.php/faqs>



remedy any breach or take such action as may be required. NITA-U considered the petition received from the office of the Speaker of Parliament of Uganda, made by Mr. Obedgiu Sammy who alleged that Guinness Transporters Limited *trading as* SafeBoda was implicated in an investigation report by a Civil Society Organisation – Unwanted Witness, for sharing its users’ personal data without their consent. In addition to addressing the above NITA-U also sought to assess how SafeBoda applied its policies on data protection and related matters in its data processing operations for purposes of identifying their effectiveness and propose improvements if any.

2.2 Methodology

2.2.1 Planning

Notice of the investigation was communicated to the SafeBoda Chief Executive Officer to inform him of the background to and purpose of the investigation. Another notice of investigation was sent to Unwanted Witness and a separate one to the petitioner (Mr. Obedgiu).

An entry meeting was held with representatives of SafeBoda management on 3rd September 2020 whereat the complaint was discussed and the planned onsite investigation process was communicated and agreed. Another entry meeting was held with Unwanted Witness representatives on 10th September 2020 whose discussion premised on their investigation report on the matter at hand and the methodology they used.

2.2.2 Collection of information for review

2.2.2.1 Documentation

Between 2nd October, 9th and 12th November 2020 SafeBoda submitted to NITA-U documentation governing its personal data processing operations. On 24th September 2020 NITA-U also received a copy of the investigation report from Unwanted Witness which was relied on by the petitioner to make his complaint. The documents were analysed by



NITA-U and interviews scheduled to obtain clarity on them and to establish how they are applied at SafeBoda in its personal data processing operations.

2.2.2.2 Interviews

SafeBoda management including staff in charge of personal data processing operations were interviewed on 5th, 10th and 16th November 2020 on the availability and content of documents supporting data protection policies, procedures and processes. They were also interviewed with respect to the applicability of the said policies in SafeBoda's personal data processing operations.

The petitioner was interviewed on 21st October 2020 with respect to the petition against SafeBoda. He informed NITA-U that attempts were made to reach SafeBoda management to rectify the gaps in its personal data processing operations as highlighted by the Unwanted Witness investigation report, but this was to no avail hence his filing the petition with the office of the Speaker of Parliament of Uganda.

3. INVESTIGATION FINDINGS

In relation to the investigation, NITA-U made the findings of fact on the balance of probabilities as guided by *Lancaster v. Blackwell Colliery Co. Ltd 1918 WC Rep 345* and *Sebuliba v. Cooperative Bank Ltd [1982] HCB 130*. NITA-U evaluated the evidence to establish the following:

- i) Whether the 2017 Data Privacy Policy and 2019 Data Protection Policy named the recipients with whom SafeBoda will share its users' personal data?
- ii) Whether SafeBoda unlawfully disclosed its users' personal data?



- iii) Whether the data processing contract between SafeBoda and CleverTap adheres to the security measures specified under the Data Protection and Privacy Act, 2019?
- iv) Whether SafeBoda applied its Data Protection policy in its personal data processing operations?

3.1 Whether SafeBoda’s 2017 Data Privacy Policy and 2019 Data Protection Policy named the recipients with whom SafeBoda will share its users’ personal data?

Within the 2017 SafeBoda Privacy Policy clause on third-party disclosure, it is provided that personally identifiable information shall be disclosed to website hosting partners and other parties who assist SafeBoda in operating its website, conducting its business or serving its users. Clause 12.2.5 of the 2019 Data Protection Policy stipulates that information shall be provided where the personal data is to be transferred to one or more third parties.

NITA-U evaluated SafeBoda’s 2017 and 2019 Data Protection policies against the statutory requirement for a data controller to provide certain information to data subjects before collection of their personal data including among others information on recipients with whom their personal data will be shared. This evaluation was based on Section 13 of the Data Protection and Privacy Act, 2019 (hereinafter referred to as “the Act”). SafeBoda submitted to NITA-U the evaluated policies on 9th November 2020.

Conclusion

The SafeBoda Privacy Policy and Data Protection Policy versions of 2017 and 2019 respectively did not provide information on recipients with whom its users’ personal data will be shared. This shows that SafeBoda did not address this non-compliance pointed out by an investigation report authored by Unwanted Witness and the petitioner. It was noted that SafeBoda made an effort to improve its adherence to this requirement with regards to its 2020



policy which it plans to upload to its application at the conclusion of this investigation.

3.2 Whether SafeBoda unlawfully disclosed its users' personal data?

In a software code and data processor personal data sharing practices review session with SafeBoda held on 16th November 2020, it was established that SafeBoda shared its users' personal data with CleverTap – a data processor that offered Software as a Service for customer lifecycle management and mobile marketing. The categories of user information shared included:

- i) E-mail address;
- ii) Mobile device Operating System;
- iii) Telephone number;
- iv) Application version;
- v) First and last names;
- vi) Mobile device name;
- vii) Application type; and
- viii) User log in status.

The access to this data was managed through accounts that required creation of a username and password by SafeBoda with access levels specified in accordance with user roles e.g. marketing and technical support.

SafeBoda further confirmed to NITA-U during the interviews conducted on 10th November 2020 that the sharing of the personal data was based on users' consent obtained during the registration process after downloading the SafeBoda application and was for analysis purposes.

NITA-U assessed whether the above "consents" were specific and informed (as required by Section 2 of the Act) on the details of recipients with whom SafeBoda users' personal data will be disclosed to. On 16th November 2020



NITA-U analyzed a sample consent database of SafeBoda users for the period from June to November 2020.

Conclusion

NITA-U's finding is that SafeBoda's disclosure of its users' personal data to CleverTap contravened the Data Protection and Privacy Act since the 'consents' relied upon for the disclosure were not specific neither were they informed, given that the users were not informed of a) the extent of the personal data collected and b) the potential disclosure of their personal data with CleverTap. There was no evidence found to support allegations that SafeBoda sells its users' personal data.

3.3 Whether the data processing contract between SafeBoda and CleverTap adheres to the security measures specified under the Act

SafeBoda shared with NITA-U a copy of the data processing contract/ subscription order that was executed on 1st January 2020 between SafeBoda Holding in Mauritius and CleverTap. During the interviews conducted on 10th November 2020 SafeBoda informed NITA-U that the purpose of the contract was to enable it access CleverTap's platform to share users' events with CleverTap for behavioural analysis. The SafeBoda team defined an event to mean any data of the corresponding end user recorded when a SafeBoda user performs an action on the application, such as clicking on the Data Protection Policy, making a request for a rider, amongst others.

It was observed that CleverTap in its "Terms of Use" included in the contract committed to ensuring confidentiality of personal data shared with it. This was in compliance with one of the requirements under Section 21 of the Data Protection and Privacy Act on establishing and maintaining confidentiality of personal data shared with a data processor.

Conclusion



Much as SafeBoda's contract with CleverTap had a provision on maintaining confidentiality of personal data shared with it, there were no other security measures included to ensure integrity of the data as required by Section 21(2) of the Data Protection and Privacy Act.

3.4 Whether SafeBoda applied its Data Protection policy in its personal data processing operations

a) Governance

SafeBoda informed NITA-U in a letter dated 2nd October 2020 that it had designated the role of Data Protection Officer to its senior management team headed by Mr. Maxime Dieudonné, the director and co-founder.

During interviews with SafeBoda conducted on 5th November 2020 NITA-U established that data protection matters were reported to the highest level of management (the board). This was corroborated by documentary evidence of e-mail extracts submitted by SafeBoda on 9th November 2020. It was also reiterated during the interviews that the senior management team was the designated Data Protection Officer as required by Section 6 of the Act. It was further established that the said team is supported by external counsel – KTA Advocates.

Conclusion

SafeBoda had designated its senior management team headed by Mr. Maxime Dieudonné as the Data Protection Officer to ensure compliance with the Act as required by Section 6 of the Data Protection and Privacy Act.

b) Information notices/policies/statements/disclosures

On 9th November 2020 SafeBoda submitted its 2019 and 2020 versions of Data Protection policies.



At the interviews held on 10th November 2020 SafeBoda informed NITA-U that the 2019 version covered its data processing operations for the subsequent period while the 2020 version was still in draft form. NITA-U reviewed both versions against the information requirements specified in Section 13 of the Data Protection and Privacy Act to establish their adherence to them. The requirements cover the following areas:

- i) Nature and category of personal data collected;
- ii) Name and address of person responsible for data collection;
- iii) Purpose for which the data is required;
- iv) Legal basis of processing;
- v) Details of persons with whom data is shared;
- vi) Data subject rights;
- vii) How long the data is retained, amongst others.

Conclusion

The 2019 and 2020 Data Protection policies lacked information on the following:

- i) Details of recipients with whom SafeBoda will share its users' personal data;
- ii) Nature and category of personal data collected (such as data provided by a user at registration and other data collected by automated means through channels like cookies); and
- iii) Legal basis for each category of personal data collected.

The 2019 policy also lacked information on purpose for which the data is collected. It was observed that the 2020 version of the policy was an improvement in comparison to the 2019 version, however, to bring it to full compliance with Section 13 of the Act, our recommendations provided in this report should be adopted.



c) Access to personal information requests and other data subject rights

On 10th November 2020 SafeBoda informed NITA-U that queries and complaints from its users were handled within its Customer Relationship Management tool.

SafeBoda further informed NITA-U during the 10th November 2020 interviews that it had not received any access to personal information requests from its users. However, it made representations that a number of personal data rectification requests were received and handled within its Customer and Relationship Management processes and procedures. It was also established that the effectiveness of these processes and procedures were evaluated on a weekly basis against the institution's targets.

Conclusion

It was established that SafeBoda's complaints and queries handling processes and procedures were fully documented, implemented and reviews were conducted to assess the effectiveness of the controls in place. However, the processes need to be improved by making provision for the statutory response timelines prescribed by Section 24(9) of the Data Protection and Privacy Act.

d) Incident response/ breach management

In representations made to NITA-U on 10th November 2020, it was established that SafeBoda's personal data incident response/ breach management processes and procedures were ad hoc in nature – meaning they were generally informal.

Section 23 of the Act requires that a data controller, data processor or data collector must immediately notify NITA-U of any personal data security breach. Institutions are expected to have in place procedures, approved and endorsed by the highest level of management, for dealing with any personal data security breaches.



Conclusion

SafeBoda's incident response/ breach management processes and procedures for personal data security breaches were not fully documented. This may negatively affect the institution's ability to detect and immediately notify both the institution's Data Protection Officer and NITA-U of any personal data security breaches it becomes aware of as required by Section 23 of the Data Protection and Privacy Act.

e) Awareness and training

On 2nd October 2020 SafeBoda submitted a presentation on ethics training that it had earlier made to its employees. Another presentation on data security conducted in August 2020 was also shared on 9th November 2020.

The accountability principle under Section 3(1)(a) of the Act requires institutions to demonstrate that they comply with the principles of the Act. As part of demonstrating compliance, it is essential to inform and train members of staff on the institution's data protection policies on how to manage risks presented by the institution's processing activities and their obligations under the Act.

Conclusion

SafeBoda made an effort to create awareness and train its employees on data protection and privacy, however, records of when and which training each member of staff took were not shared with NITA-U to verify this assertion. It was further observed from the training on ethics that the content on data protection was insufficient. This was corroborated by the limited knowledge on data protection that some of the SafeBoda staff exhibited when engaged by NITA-U on 10th November 2020.



4. RECOMMENDATIONS

Having arrived at the above findings, SafeBoda is directed to address the above areas of non-compliance by implementing the recommendations below. SafeBoda will be required to complete an action plan indicating how, when and by whom the recommendations will be implemented.

4.1 Provision of details of recipients with whom SafeBoda will share its users' personal data.

SafeBoda should update its privacy notices/policies/statements or disclosures to provide its users with information on parties it may disclose their personal data to. These recipients should be named or the categories of recipients be provided. In accordance with the principle of fairness under Section 3(1)(b) of the Act, SafeBoda must provide information on the recipients that is most meaningful for its users. In practice, this will generally be the named recipients, so that users know exactly who has their personal data. If SafeBoda opts to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients. For the named recipients that process data outside Uganda (such as CleverTap), information should be provided to the user on how this offshore processing of their personal data is compliant with the Data Protection and Privacy Act.

4.2 Disclosure of SafeBoda users' personal data.

Since SafeBoda relies on its users' consent received during the registration process to share their personal data, it is vital that such consent is specific and informed. Once this condition is met, then the sharing or disclosure of its users' personal data to recipients like CleverTap can be deemed to be in accordance with the Data Protection



and Privacy Act, 2019. For these 'consents' to be specific and informed, the users have to be informed within the data protection notices/policies/statements/disclosures that their personal data will be shared with CleverTap or with any institution of a similar nature for purposes of user/customer lifecycle management and mobile marketing or any other purpose determined by SafeBoda. SafeBoda is encouraged to develop a method to demonstrate that valid consent was obtained before collection of its users' personal data to enable the institution to lawfully disclose the data to other parties. For instance, SafeBoda may keep a record of consent statements received, so it can show how consent was obtained, when consent was obtained and the information provided to the users at the time.

4.3 Align contract between SafeBoda and CleverTap with Data Protection and Privacy Act.

The contract between SafeBoda and CleverTap should be amended to enable the former demonstrate implementation of appropriate security measures relating to data processed by a data processor as required by Section 21 (2) of the Act. This should be reflected in the contract to include the following:

- i) SafeBoda's and CleverTap's respective obligations;
- i) appropriate security measures to be adopted by CleverTap;
- ii) requirement for CleverTap to notify SafeBoda before engaging any sub-processors;
- iii) end-of-contract provisions on handling of shared data; and
- iv) requirement that SafeBoda can audit CleverTap or have access to an external auditor's attestation on status of security measures.

The aforementioned contract should be further amended to enable SafeBoda demonstrate to its users as required by Section 3(1)(a) of the



Act the accountability principle regarding their personal data collected and processed. This principle should be reflected in the contract to include the following:

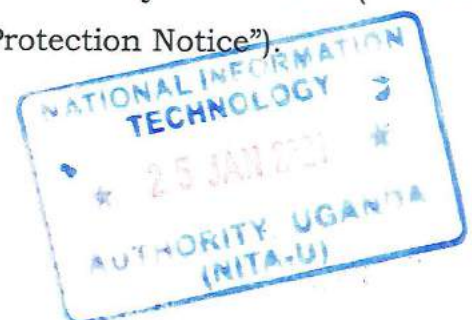
- i) subject matter of the processing;
- ii) nature and purpose of the processing; and
- iii) the type of personal data processed and categories of data subjects covered by the processing.

4.4 Application of Data Protection policy in SafeBoda's personal data processing operations

4.4.1 Information notices/policies/statements/disclosures.

The 2020 Data Privacy Policy should be updated to include information on recipients with whom SafeBoda will share its users' personal data. It should also state whether the supply of data by the users is discretionary or mandatory and consequences of failure to do so [Section 13(1)(d) - (f) of the Act]. Additionally, it should specify the safeguards in place for the cross-border transfer of personal data, especially where consent of the users will be relied on as the basis for the transfer (Section 19 of the Act). If SafeBoda performs automated decision-making (including profiling), the envisaged consequences of such processing for the users should be provided (Section 27 of the Act). The right to lodge a complaint with regulator - Personal Data Protection Office should be stated and other rights, such as the right of access to data collected, right to request rectification of data collected should equally be provided for therein.

The updated policy should be published on the website and mobile application. A direct link to this policy should be clearly visible on each page of the website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice").



For the mobile application, the necessary information should also be made available from an online store prior to download. Once the application is installed, the information still needs to be easily accessible from within the application.

SafeBoda should also include the version and date of the current policy in order for a data subject confirm the updates and changes made or provide assurance that the published privacy notice is the current version.

4.4.2 Access to personal information requests and other data subject rights.

SafeBoda's Customer and Relationship Management tool should be configured to cover the statutory response timelines prescribed by Section 24(9) on access to personal information requests and other data subject rights under Part V of the Act.

4.4.3 Incident response/ breach management.

SafeBoda should update the "Employee Handbook" to include a process for reporting personal data security breaches to the Data Protection Officer and also communicate consequences for failure to do so. Beyond ensuring the process is fully documented, SafeBoda should ensure that it is implemented and reviews conducted to assess its effectiveness. This will enable SafeBoda to detect and immediately notify the Personal Data Protection Office of any personal data security breaches it becomes aware of as required by Section 23 of the Data Protection and Privacy Act.

4.4.4 Awareness and training.

The Data Protection Officer is advised to raise awareness and train staff that handle personal data about the Data Protection and



Privacy Act and the institution's Data Privacy Policy. Documentation showing the content and delivery of the training and awareness conducted should be maintained on record. Awareness should be created to the SafeBoda application users about their rights as provided by the Data Protection and Privacy Act in as far as collecting and processing their personal data.

The training manuals for staff awareness and training should be updated to include specific provisions on obligations of staff for personal data protection and data security best practices. This should further be supported by development and implementation of an awareness and training plan that will describe the frequency, the channels to be used, mandatory participation of all staff and templates to record attendance.

4.4.5 Internal-facing Data Protection Policy

SafeBoda should develop an internal-facing Data Protection policy setting out the principles and legal conditions that the institution must satisfy when collecting, processing, transferring or storing personal data in the course of its operations. This document not only demonstrates how the institution processes personal data but also makes employees aware of their data protection obligations, such as how and when to respond when data subjects exercise their rights generally (and specifically in relation to access to personal information requests).

The "SafeBoda Employee Handbook" should be updated to reference the internal-facing Data Protection policy. Each member of staff should be required to sign an acknowledgment of the updated handbook in addition to availing them copies of the Data Protection policy. Additionally, the section on Disciplinary policy within the



“Employee Handbook” should be modified to include action to be taken against staff who have violated policies and procedures on data protection and the requirement to keep a record of such action taken.

5. CONCLUSION

NITA-U’s assessment is that SafeBoda’s disclosure of its users’ personal data to CleverTap contravened Section 35 of the Data Protection and Privacy Act since the 'consents' relied upon for the disclosure were not specific because they did not disclose the parties with whom the information was going to be shared with.

SafeBoda was cooperative during the investigation and has also made the following efforts towards improving its compliance with the Data Protection and Privacy Act, 2019:

- i) An improved Data Protection and Privacy policy has been developed.
- ii) A Data Protection Officer was designated to ensure compliance with the Act.
- iii) Efforts were made to create awareness to its staff on provisions of the Act.

We also observed that SafeBoda had already made efforts to adhere to best Data Protection practices even before the law was in place when it had a Data Protection policy uploaded on its platforms in 2017.


SafeBoda is directed to address all the areas of non- compliance identified above within 4 months from the date of issue of this report. To enable the Authority monitor implementation of the above directions, SafeBoda is required to submit an action plan for implementing the actions within two (2) weeks from the date of issue of this report. In the event SafeBoda does not



implement the measures identified above, the Authority reserves its right to commence prosecution under S.35 of the Data Protection and Privacy Act.

Dated the 25th day of January 2021

Signed



DR. HATWIB MUGASA

Executive Director

National Information Technology Authority, Uganda (NITA-U)



ANNEXURES



ANNEX "A"
**PETITION TO OFFICE OF THE SPEAKER OF
PARLIAMENT AGAINST GUINNESS
TRANSPORTERS LIMITED**



Amul Central
Sign + advice
all/hrs

21 JUL 2020

Hon. Rebecca Kadaga
Speaker of parliament
Republic of Uganda
Parliament Avenue
Kampala

21 JUL 2020

20th July, 2020

Re: Petition against Guinness Transporters limited trading as Safe boda selling/sharing Ugandan's Data with American big tech companies like Facebook.

An NGO called Unwanted Witness Uganda last week released a report implicating SafeBoda – a motorcycle transport company that operates in Uganda, Kenya and Nigeria – in sharing their client's personal data with third parties without their knowledge or permission as required by Section 7 of the Data Protection and Privacy Act of Uganda, raising legal issues as well as questions of trust.

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. Uganda become the first country in East Africa to enact the data protection law. We are scared that if companies like safe boda don't abide by the principles espoused in this law, our national security could be at risk, like we saw recently in 2016 when Russians meddled in the 2016 American presidential elections.

Unwanted witnesses carried out forensic research about SafeBoda's privacy policy and its practice. When reviewing their privacy policy and comparing it to how the app actually operates, a number of discrepancies were identified.

It was 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 a Software Development Kit (SDK). Through this SDK, Facebook routinely collected information on SafeBoda's users via the SafeBoda app.

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.

Following unwanted witnesses communication with SafeBoda asking for clarification, they removed Facebook trackers from the application.

0780448012
sammyubedgi@gmail.com



Safeboda then proceeded to install a new tracker CleverTap. This App provides mobile app analytics – this means that every time a user uses the SafeBoda app, it still sends users' data to CleverTap, a third-party, without their consent.

It is not the first time CleverTap has been involved in cases of sharing users' data without their consent. Privacy International, a charity based in London that works at the intersection of modern technologies and rights, discovered this tracker in menstruation applications. The users' data that's shared include: the user's phone type, phone contact number, email address, location, time-zone, user-names, and their carrier (Internet Service Provider)

As a petitioner, I therefore parliament to implore NITA-U, TO use SafeBoda as an example to get other data collectors to make adjustments to meet the required data protection standards and principles:

- *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*
- *Safeboda should have clear comprehensive privacy policies and these should be strictly enforced.*
- *The company should exhaustively specify the third-parties and the exact personal data it shares with them in its privacy policy.*
- *It is recommended that efforts be taken to establish "pathways" that can be followed by data subjects to allow them, if interested, to understand how their personal data may be being processed by the company and any third parties.*

For the sake of national security, safeboda might not be an innocent transportation company its an aggressive processor of Ugandans data to sell it to big tech American companies that are under investigation by their own congress. It's no surprise that the U.S Department of Justice is bringing anti-trust violations against big tech companies in a bid to break them up.

Data in 2017 surpassed the value of oil, its now a trillion dollar industry. We implore parliament not to take this for granted.

Attached is the detailed findings of the report by the Unwanted witnesses NGO

LEAD PETITIONER

Sammy Obedgiu

OBEDGIU SAMMY

0780448012
sammyobedgiu@gmail.com



ANNEX “B”
UNWANTED WITNESS’ INVESTIGATION
REPORT



SAFEBODA TECH RESEARCH

Research Methodology for Dynamic Analysis

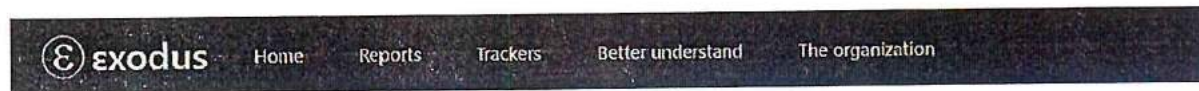
We conducted a dynamic analysis of the apps, using the following components:

- A laptop running a Virtual Machine (using Oracle's VirtualBox) with mitmproxy in "transparent" mode (meaning that the connection is being intercepted without the knowledge of the client). Along with the necessary tools to create a functional network access point. The Virtual Machine is running Debian 10 (Buster)
- Android Phones, Running Android Oreo (for the initial analysis) and Android 6 (for the latter analysis)

All data being transmitted between third parties and apps is encrypted in transit using Transport Layer Security (TLS, formally SSL). Our analysis consisted of capturing and decrypting data in transit between our own device and third party servers (so called "man-in-the-middle") using the free and open source software tool called "mitmproxy", an interactive HTTPS proxy. Mitmproxy works by decrypting and encrypting packets on the fly by masquerading as a remote secure.

In order to make this work, we added mitmproxy's public key to our device as a trusted authority. The data exists on our local network at time of decryption.

FINDINGS FROM THE INITIAL ANALYSIS



SafeBoda

6 trackers

8 permissions

Version 3.2.4 - [see other versions](#)

Source: Google Play

Created by: SafeBoda Holding

Downloads: 500,000+

Report created on Sept. 13, 2019, 3:15 p.m. and updated on July 14, 2020, 4:43 a.m.

[See on Google Play](#) >

6 trackers

We have found code signature of the following trackers in the application:

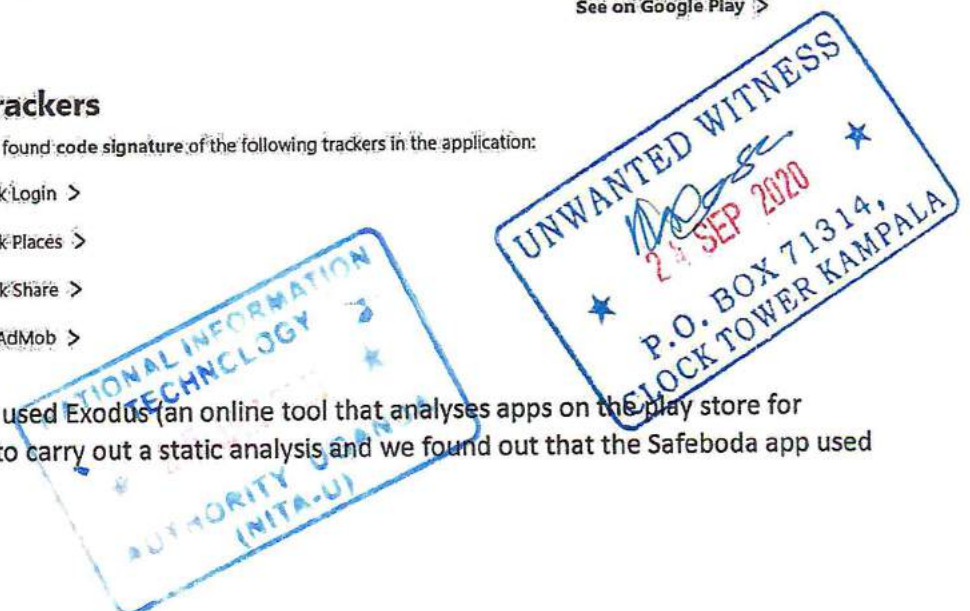
Facebook Login >

Facebook Places >

Facebook Share >

Google AdMob >

From the figure above, we used Exodus (an online tool that analyses apps on the play store for trackers and permissions) to carry out a static analysis and we found out that the Safeboda app used Facebook trackers.




```

Request  Response  Details
POST https://graph.facebook.com/v4.0/643188935803637/activities HTTP/1.1
User-Agent          FBAndroidSDK.5.2.0
Accept-Language     en_GB
Content-Type        application/x-www-form-urlencoded
Content-Encoding    gzip
Transfer-Encoding   chunked
Host                graph.facebook.com
Connection          Keep-Alive
Accept-Encoding     identity

format:            json
sdk:               android
event:             MOBILE_APP_INSTALL
advertiser_id:     4a75c883-9fb3-4b1f-97bd-1f95910b8cec
advertiser_tracking_enabled: true
installer_package: com.android.vending
anon_id:           XZcaf3ab0c-1eb8-450a-a697-e3d45f53cdfc
application_tracking_enabled: true
extinfo:           ["a2","com.safeboda.passenger",3092004,"3.2.4","9.1.0","Pixel","en_GB","GMT+03:00","Safaricom",1080,1794,"2.62",4,24,16,"Africa/Nairobi"]
application_package_name: com.safeboda.passenger

```

The screenshot above was extracted from our testing environment when we carried out a dynamic analysis on the Safeboda application. In the second last field (extinfo) from the screenshot, the application shared the user's android version, screen-size, location, phone type, time and the internet Service Provider to graph.facebook.com.

NOTE: The first analysis was carried out in Nairobi, Kenya.

FINDINGS FROM THE RECENT ANALYSIS.



SafeBoda

5 trackers

11 permissions

Version 3.3.15 - [see other versions](#)

Source: Google Play

Report created on June 18, 2020, 12:52 p.m. and updated on July 13, 2020, 9:51 p.m.

[See on Google Play >](#)

5 trackers

We have found code signature of the following trackers in the application:

[Amplitude >](#)

[CleverTap >](#)

[Google AdMob >](#)

[Google Crashlytics >](#)

[Google Firebase Analytics >](#)

A tracker is a piece of software meant to collect data about you or your usages. [Learn more...](#)

After sending our findings to Safeboda, the Facebook trackers were removed from the application. From the screenshot above, Safeboda added another two new trackers namely; CleverTap and Amplitude.



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",
      "Co": "UG",
      "dpi": 320,
      "hgt": 4,
      "useIP": false,
      "wdt": 2.25
    },
    "ait": 0,
    "arp": {
      "av": "3.3.11",
      "d_ts": 1584696716,

```

The screenshot above was extracted from our testing environment. The Safeboda application used the wzrkt.com tracker (a tracker owned by CleverTap) to transfer the user's information like Carrier, phone make, phone model, OS version and others without user's knowledge.

```
{
  "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 proto 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",

```

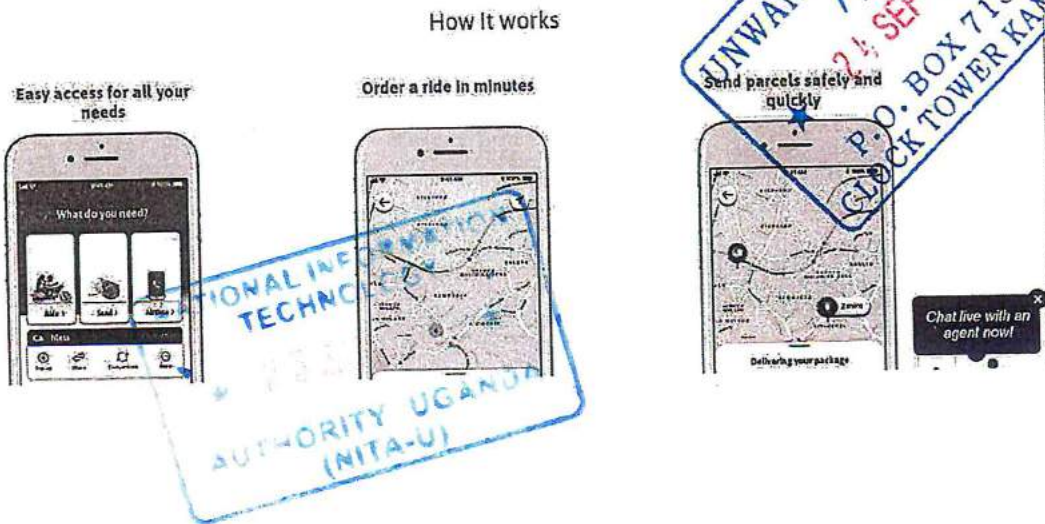
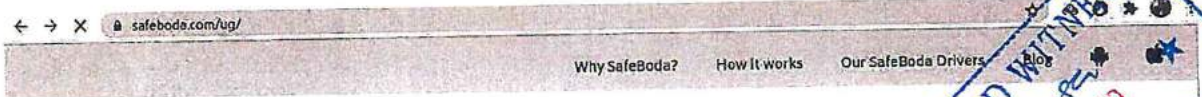
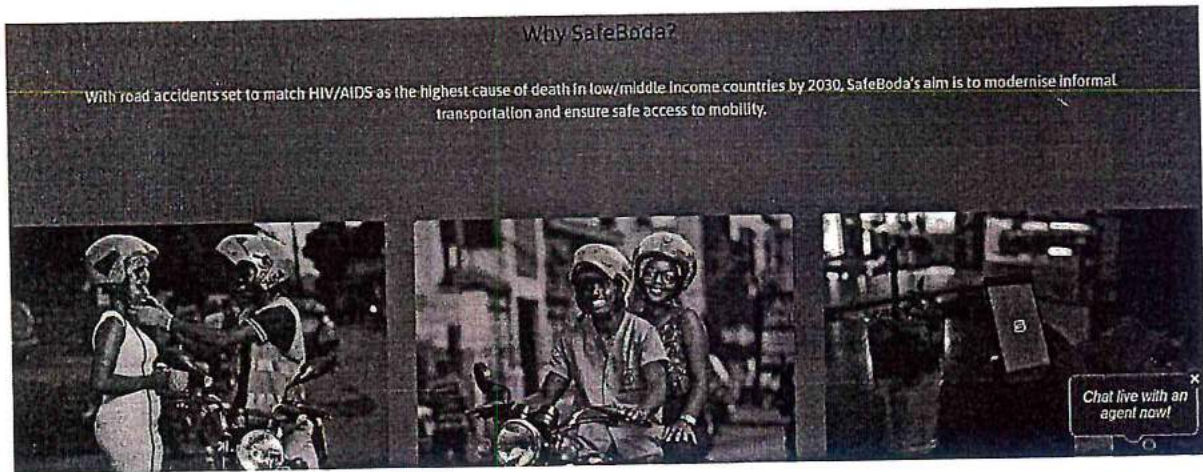


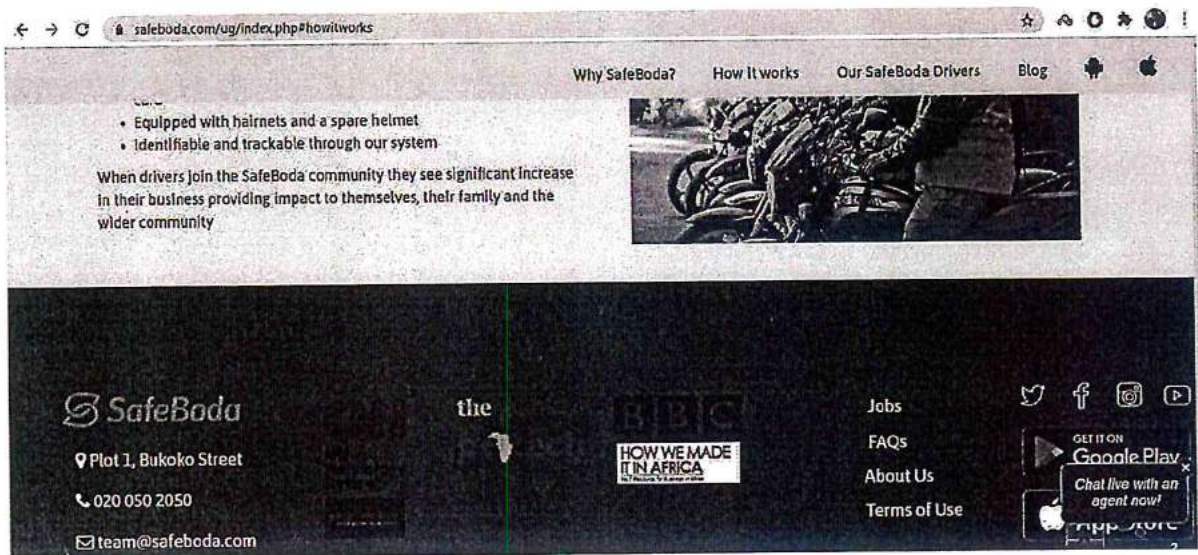
The tracker went ahead to transmit the above information including the user's source and destination GPS coordinates to CleverTap.



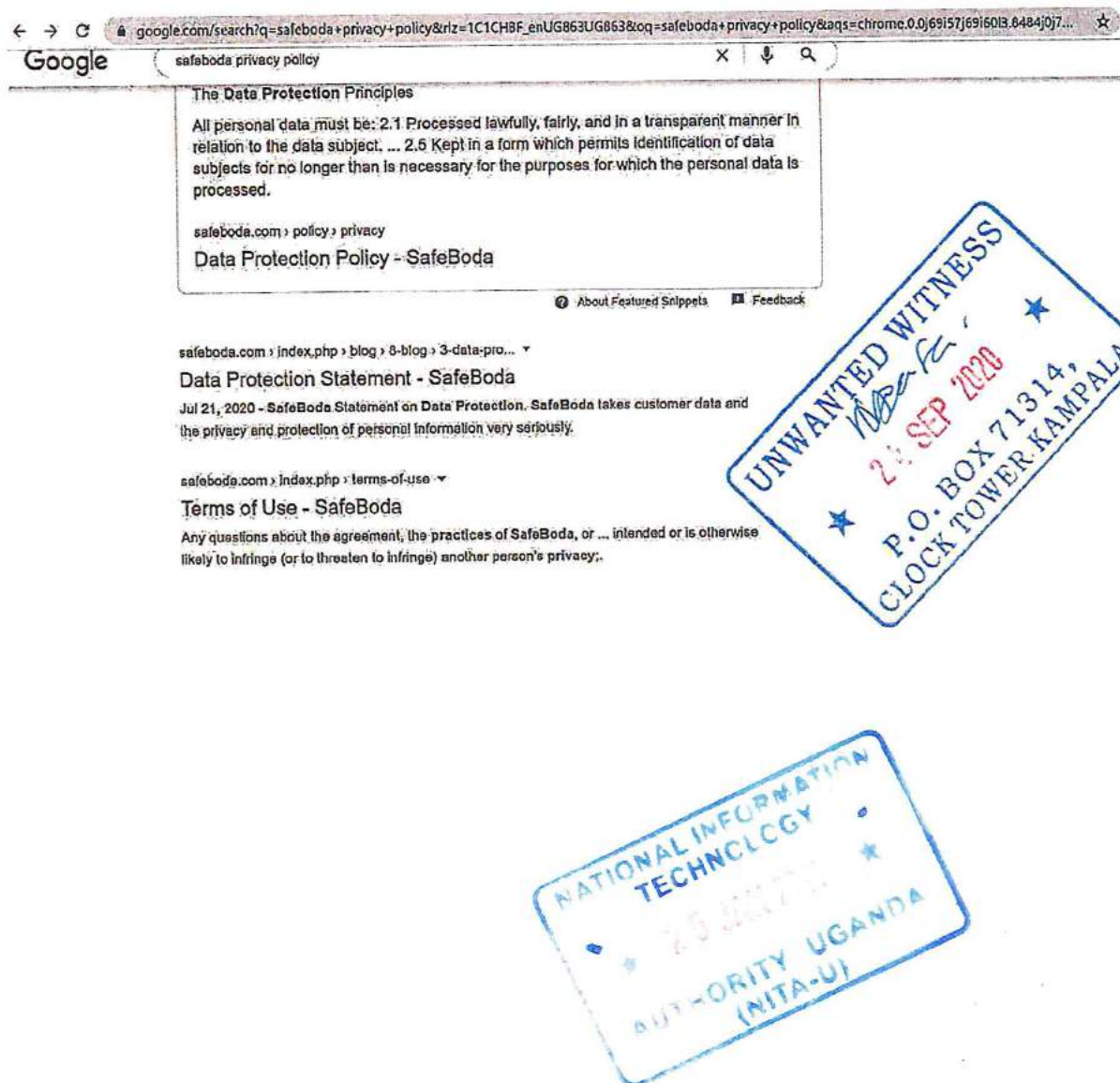
HIDDEN PRIVACY POLICY

The privacy policy of the company isn't on the front page.

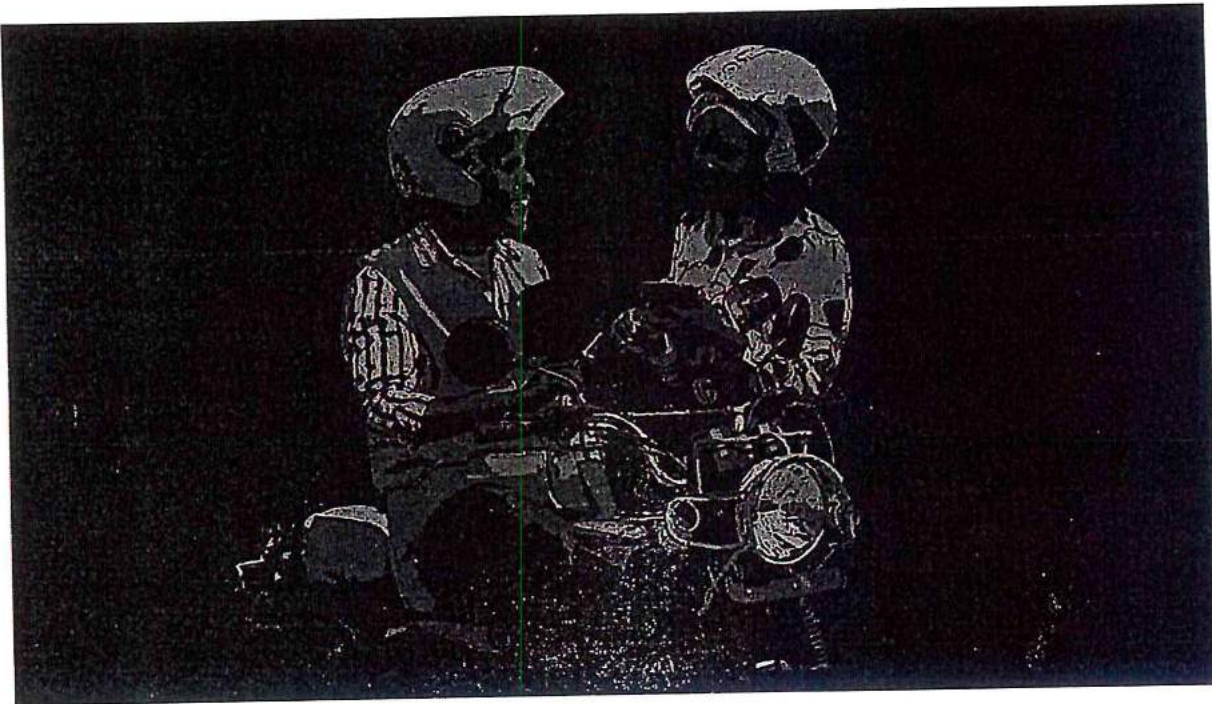




A user has to use a search engine like "Google" to access the company's privacy policy; the privacy policy could only be accessed if a user submitted terms like "Safeboda Privacy Policy" into the Google search engine.



TRADING PRIVACY FOR A CHEAP TRANSPORT SYSTEM



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:

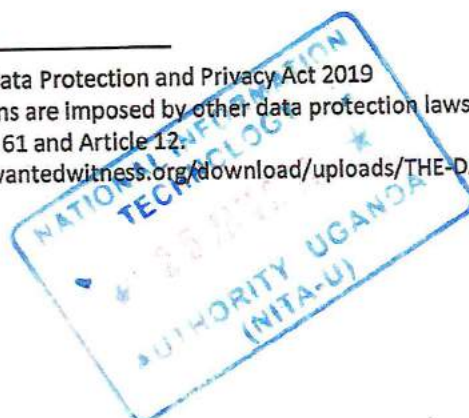
It is a legal requirement for companies to inform individuals who use their products and services about how their data is being processed¹. This is the purpose which a Privacy Policy, a legal document that guides the collection, processing, and use of the personal data serves. It should be in a comprehensive and clear language that can be easily understood by any person².

Any company's processing activities contained in their Privacy Policy must comply with Uganda's Data Protection and Privacy Act, 2019³

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>



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 Africa⁴. 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 Nigeria⁵.

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 the user reaches the destination⁶. There are over 1,000,000⁷ 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 purpose⁸.

This was addressed under Clause 12.1.2 of the new SafeBoda privacy policy that⁹:

⁴ [Safeboda.com/ug/index.php/about-us](https://safeboda.com/ug/index.php/about-us)

⁵ <https://digestafrica.com/safeboda-barcelona-daily-brief>

⁶ [https://safeboda.com>index.php>faqs](https://safeboda.com/index.php>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/>



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.

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 extract¹⁰ from the older Safeboda privacy policy¹¹, 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 them¹².

Sharing personal data with third parties

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

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



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.

Caption: Extract¹³ 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 data¹⁴

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 principles¹⁵, 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 oral¹⁶.

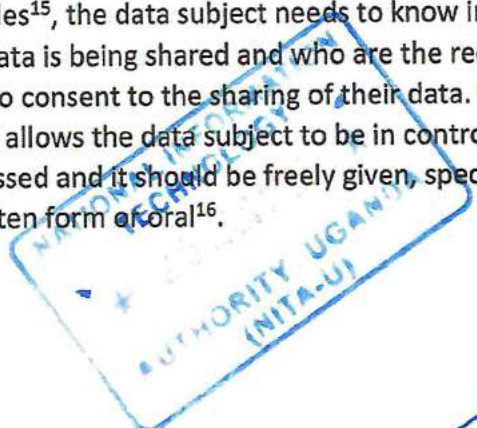
Data Retention

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



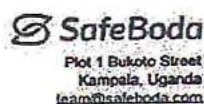
Whereas storage limitation is a key data protection principle, the previous SafeBoda privacy policy did not provide any information about the exact retention periods of personal data. It is nevertheless necessary that a data controller shall not retain the personal data for a period longer than is necessary 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 kept¹⁷.

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 retained¹⁸.

Clause 7 of the new SafeBoda privacy policy¹⁹ 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:



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

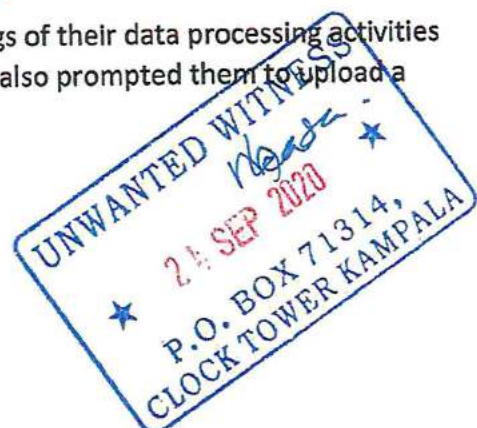


Our engagement with Safeboda over potential shortcomings of their data processing activities and the lack of clarity of their privacy policy seems to have also prompted them to upload a

¹⁷ Section 18(1) Data Protection And Privacy Act 2019

¹⁸ Section 13(1) (I), Data Protection And Privacy Act 2019,

¹⁹ <http://safeboda.com/policy/privacy/>



new privacy policy²⁰ 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 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:

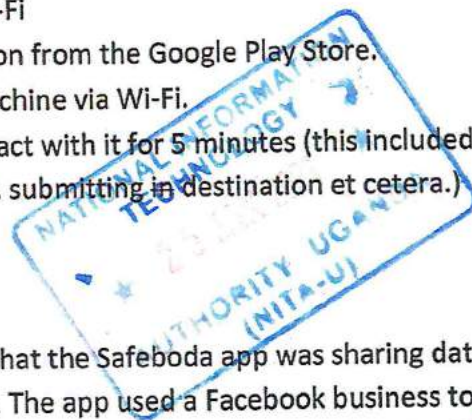
- Connect to a non-intercepting Wi-Fi
- Download the Safeboda application from the Google Play Store.
- Connect to mitmproxy Virtual Machine via Wi-Fi.
- Open the Safeboda app and interact with it for 5 minutes (this included activities like; requesting for a motorcycle rider, submitting in destination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

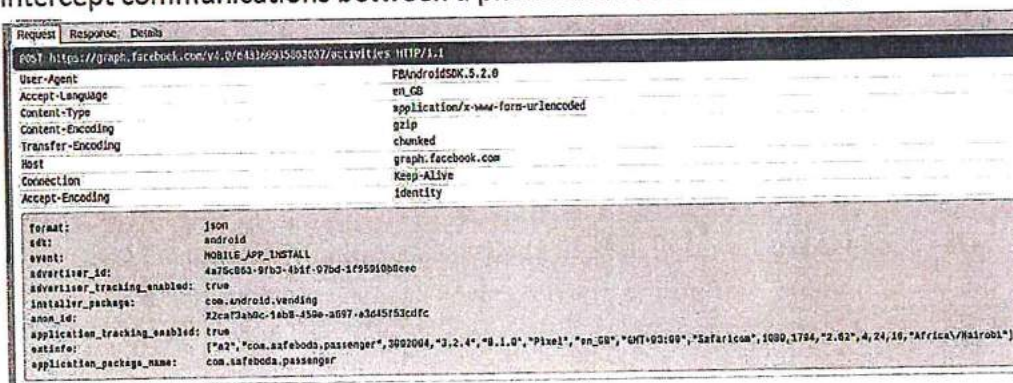
²⁰ The new privacy policy was uploaded on 4th November 2019



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 screenshot²¹ below shows an event's data that was taken from the Privacy International's data interception environment²² 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/Nairobi²³"), 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;

²¹ Taken on 2nd October 2019

²² <https://privacyinternational.org/mitmproxy19>

²³ The test was carried out in Nairobi, Kenya.



```
{
  "success": true
}
```

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. CleverTap which is formerly known as WizRocket is a SaaS-based customer lifecycle management and mobile marketing company headquartered in Mountain View, California²⁴. Founded in May 2013, it provides mobile app analytics²⁵.

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 resonates²⁶

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 applications²⁷. 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 screenshots²⁸ 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.

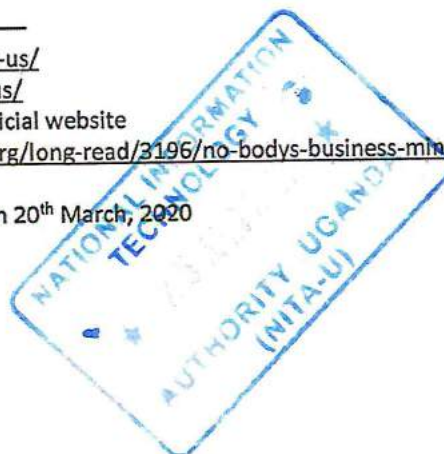
²⁴ <https://clevertap.com/contact-us/>

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://wrkt.com/api?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	wrkt.com	
Connection	Keep-Alive	
Accept-Encoding	identity	
Content-Length	1615	

```
[
  {
    "af": {
      "Build": "3060311",
      "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 Sentena 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
  },
  "evthName": "ride_estimation",
  "f": false,
  "lsl": 0,
  "pg": 1,
  "s": 1584700875,
  "type": "event",
  "wrkt_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 Sentena Rd, Kampala, Uganda",
    "from_latitude": 0.3181788,
    "from_longitude": 32.5491234
  },
  "evthName": "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.

