

# PRIVACY SCORECARD REPORT

NOVEMBER 2021

IF YOU MUST COLLECT IT,  
YOU MUST PROTECT IT.



# PRIVACY SCORECARD REPORT



---

Prepared by :  
Unwanted Witness

The Unwanted Witness is a civil society organization (CSO) that was established to respond to the gap in effective communication using various online expression platforms.

# Inside

## Privacy Scorecard Report | 2021

01   ABOUT UNWANTED WITNESS	4
02   PART 1: PRIVACY POLICY – UGANDA PERFORMANCE	6
03   PART 2: COUNTRY BENCHMARKS	11
04   PART 3: COMMON APPS IN UGANDA & TECHNOLOGY ANALYSIS	11
05   CONCLUSIONS	12
06   RECOMMENDATIONS	12
07   STUDY BACKGROUND	13
08   ABOUT THE SCORECARD – CATEGORIES AND CRITERIA	13
09   MAIN FINDINGS	20
10   REFERENCES	92

# About Us

## We are Unwanted Witness

The Unwanted Witness is a civil society organization (CSO) that was established to respond to the gap in effective communication using various online expression platforms.

Unwanted Witness was established in 2012 by a group of netizens, bloggers, activists, writers and human rights defenders as an independent, non-partisan and not-for-profit civil society organization.

It seeks to create secure uncensored online platforms for activists, netizens, bloggers, freelance journalists and writers to promote human rights through writing and informing, educating the citizenry who also utilize the platform for strengthening free expression and demand for accountability.

**Vision:** creating platforms that guarantee internet/ online freedom..

**Mission:** to contribute to good governance through effective and efficient internet/ online activism through networking and strengthening capacities of netizen for collective advocacy and synergy.

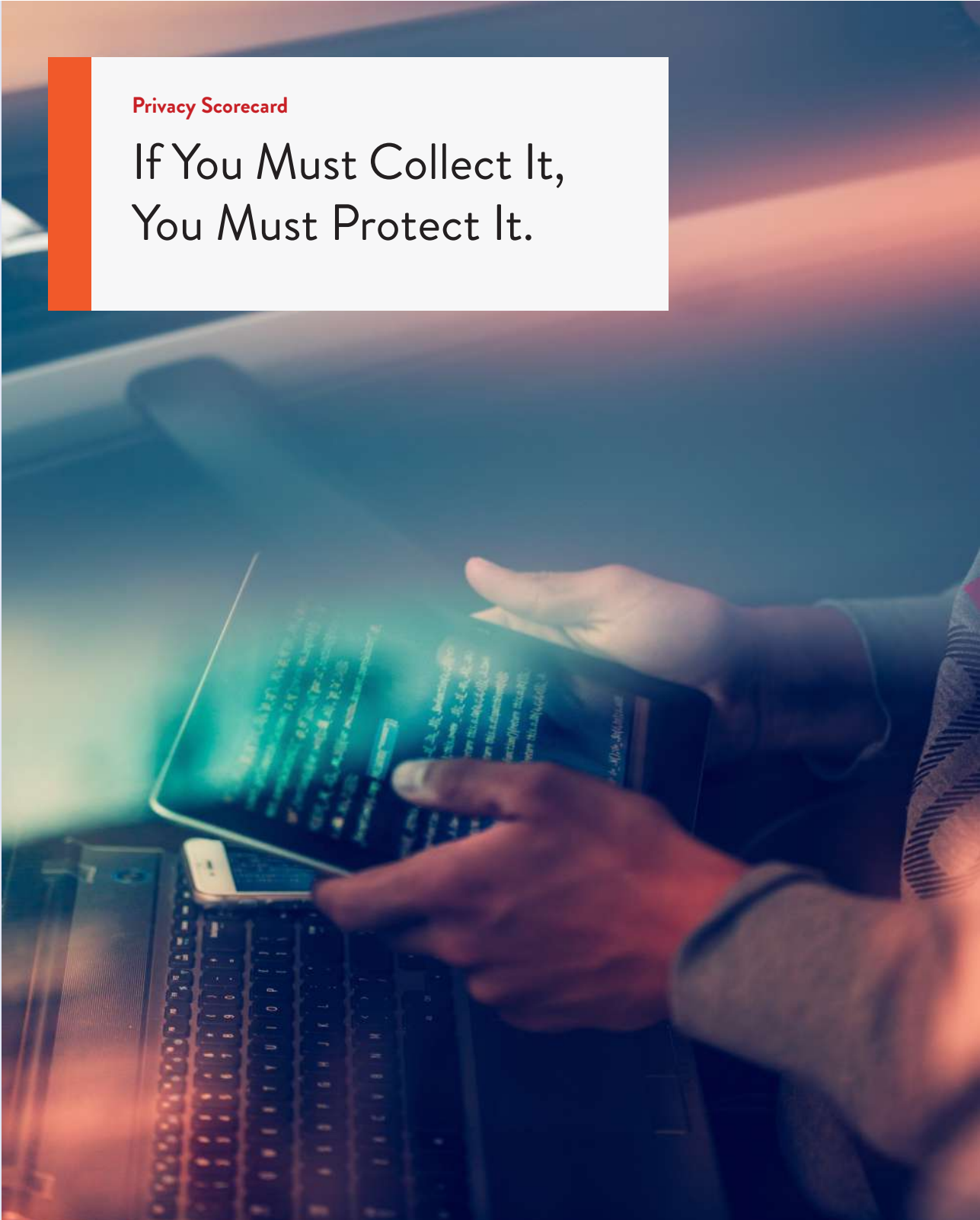


**UNWANTED  
WITNESS**

"Amplifying Voices, Changing Lives"

Privacy Scorecard Report

Prepared by : Unwanted Witness



Privacy Scorecard

If You Must Collect It,  
You Must Protect It.

# Results summary

## Index Score.

The key findings described here are based on a scorecard analysis of the research data compiled by Unwanted Witness.

The results show the extent to which different industrial and business sectors are complying with the data Protection and Privacy Act, 2019 as well as the principles and standards of data protection.

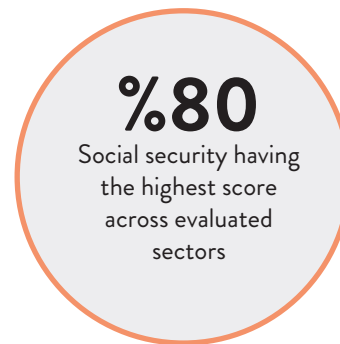
The scores vary considerably across sectors/categories, even within categories. It gives details of what these companies or organisation are doing or not doing to protect their users from potentially invasive access to their personal data.



The average performance score across all the sectors evaluated



Being the highest performing assessment criteria.

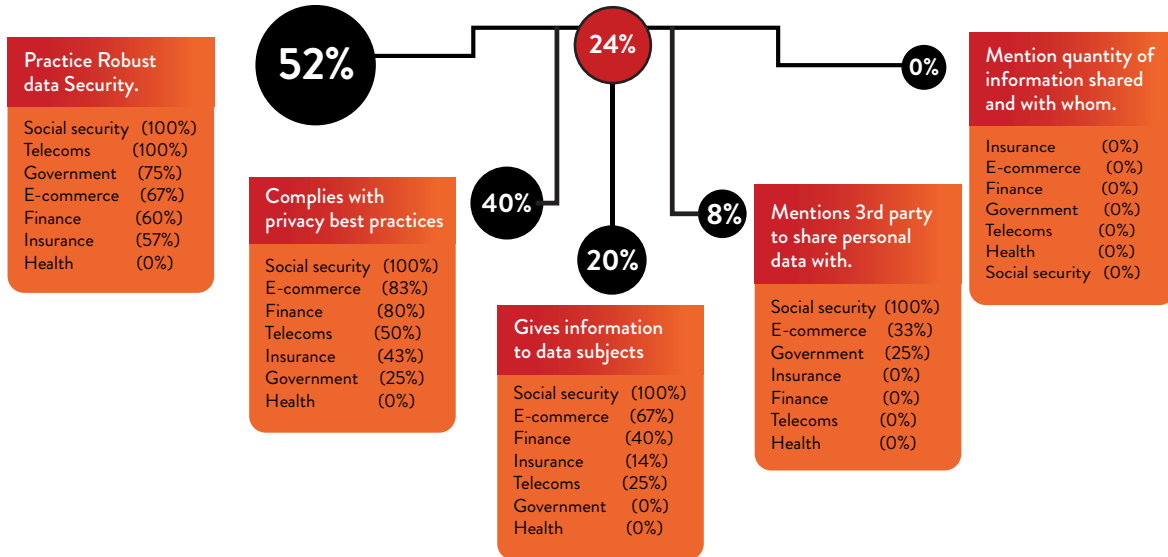


The highest score obtained across all evaluated areas by a sector



# Results Dashboard

## Index Score.



■ Social security – 80%  
 ■ E-Commerce – 50%  
 ■ Financial – 36%  
 ■ Telecom – 35%  
 ■ Govt Agencies – 35%

# Privacy Scorecard

Criteria, action and performance index

Table 1: Score per Parameters of measurement

	CRITERIA	CRITERIA	CRITERIA	CRITERIA	CRITERIA
Criteria	Complies with privacy best practices	Gives information to data subject before collection of data)	Mentions third parties with whom personal data is shared with	Practice Robust Data Security.	How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period
Action	An Accessible and Noticeable Privacy Policy)	Rights of data subjects as provided by DPPA 2019	Must mention third parties in their privacy	Their websites and apps should be secure	(A Transparency Report.)
Performance index	16	93		19	0
	54%	35%	19%	66%	0%

### EXPECTATIONS

An Accessible and Noticeable Privacy Policy)

Rights of data subjects as provided by DPPA 2019

Third parties should be mentioned

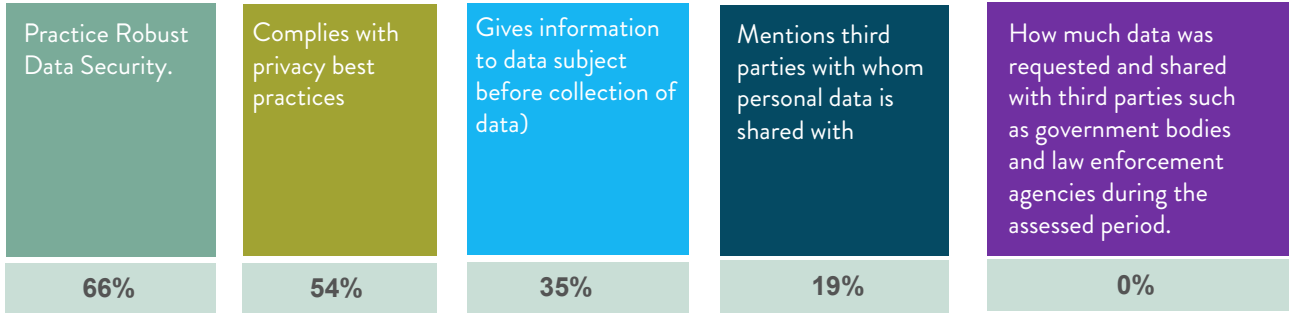
They should mention how they safeguard user data in their privacy policies.

Transparency report.



A very low score card performance (35%) is evident, a clear indication that most organisations are struggling with data protection compliance.

Highest compliance is observed for “Practice Robust Data Security” as well as “Complies with privacy best practices”. E-commerce, Financial and Telecom services register highest compliance levels. Government and insurance are also cited for practicing robust data security.



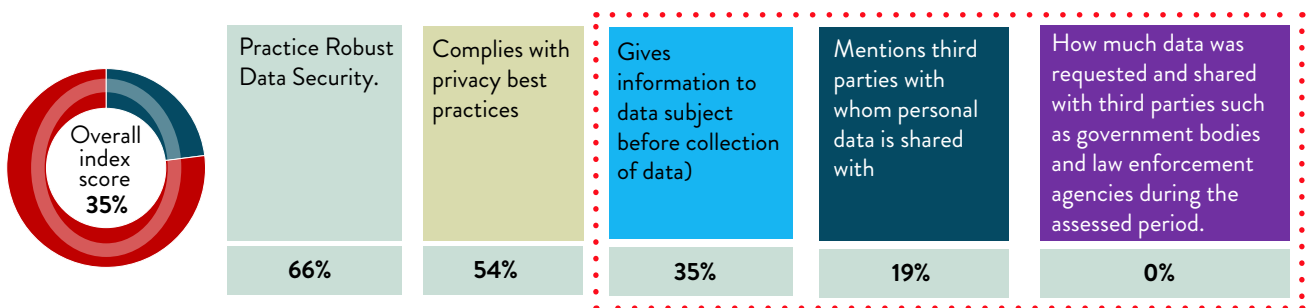
Just over half of companies/Organisations evaluated practice robust data security, evidenced with a good SSL server test results (A+, A or B), and having essential security headers. However, in some cases, this is normally compromised with existence of trackers.

A sizeable number of companies have no SSL certificates, report poor SSL server test results with no essential security headers, making them highly vulnerable to attacks.

A good number of organisations assessed have trackers on their websites sending data to companies involved in online advertising namely; Facebook, Inc. and Alphabet, Inc. (Google).

Common themes for data privacy best practices being a noticeable and accessible privacy policy at the footer of company and organisation websites, which disclose the rights of the data subjects. However, this is not consistent across all companies. In a few instances, we see the existence of privacy policy, but it may not be accessible, for example, the case of ICEA. Also, some players do not provide a complete list of the rights to data subjects, opting to provide a few options.

This incompleteness of information may be interpreted as a lack of respect to rights of data subjects and limits the control a data subject has over his information once it is transferred.



The most abused three privacy criteria, i.e., those with the least score across all categories of programs include: giving information to data subjects before collection of data (Rights of data subjects as provided by DPPA 2019)

mentioning third parties with whom data is shared and disclosure of how much data is provided to third parties including Government and law enforcement

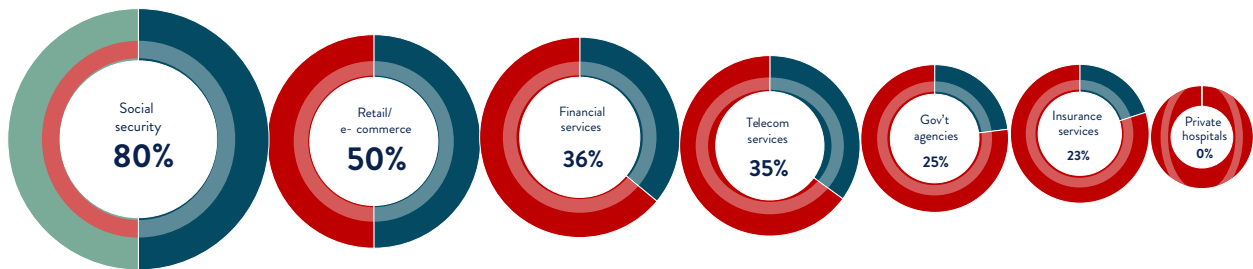
Non-disclosure of the above makes data prone to misuse



and exploitation and may be interpreted as a lack of respect to the rights of data owners. E-commerce Social Security, and to a small extent financial services players stand out for highest compliance to giving information to data subjects before collection of data, hence adherence to the rights of data subjects as provided by DPPA 2019.

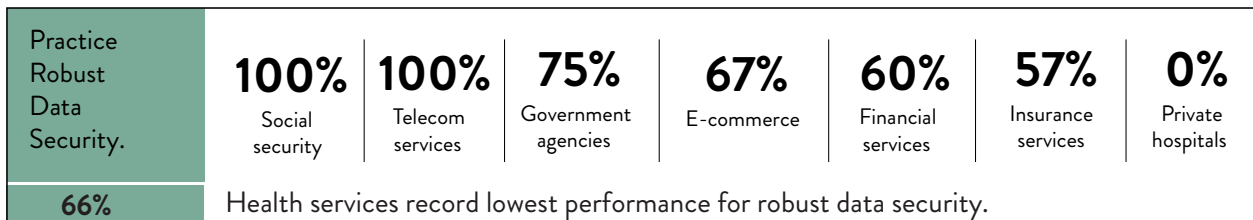
E-commerce and Social Security specifically disclose a whole range of the rights of the data subjects. Financial services performance on these aspects is worrying given that that they hold huge volumes of sensitive customer data.

Social security, and companies within the retailing/e-commerce sectors uphold the highest data protection standards. Financial and Telecoms have fair data protection practice, though the scale of practice is below expectation.

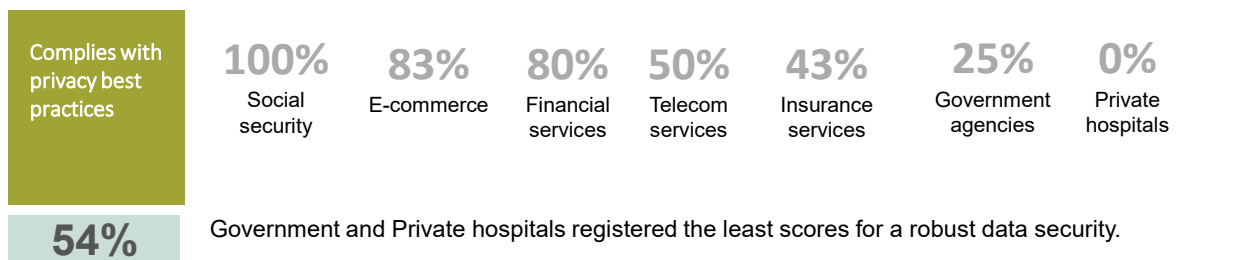


Government agencies and Insurance companies are on the tipping edge to vulnerability, while health facilities exhibit worst levels of vulnerability in compliance to data protection standards.

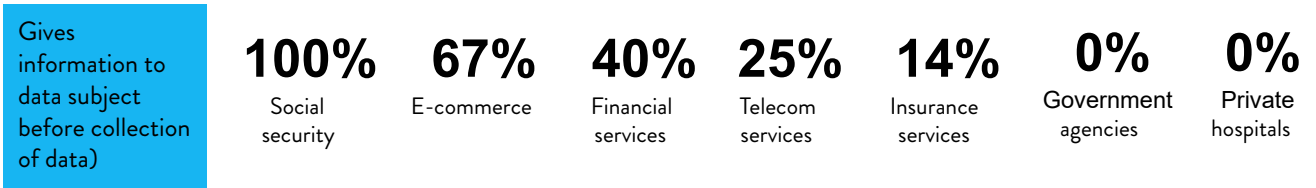
Comparatively, more sectors registered relatively good scores for practicing robust data security. Telecoms and social security lead the pack (100%), followed by government agencies, e-commerce, financial services and insurance services.



Social security (100%) and E-commerce (83%) recorded the highest score for compliance with privacy best practices. Followed by financial services (80%). Telecom and insurance service are slightly above average.



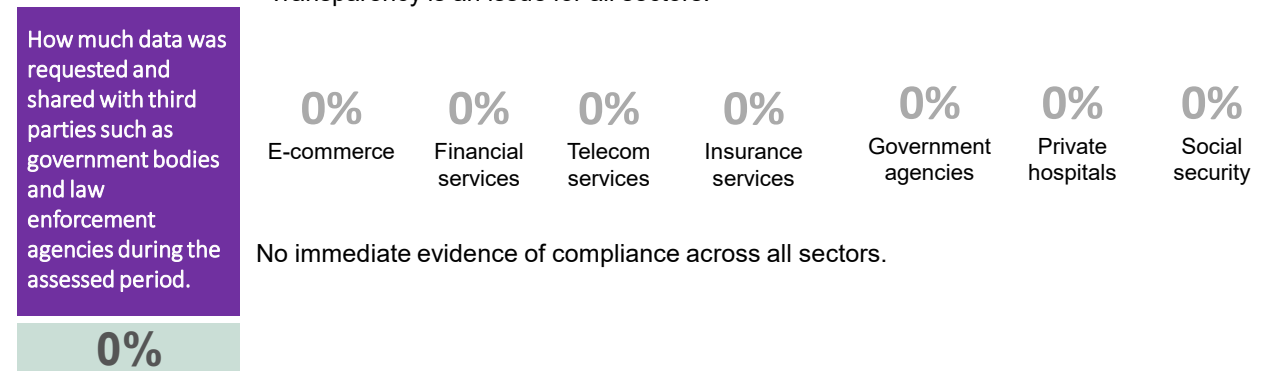
Social security(100%) and E-commerce (67%) recorded the highest score for compliance with giving information to data subjects before collection of data. Followed by financial services (40%).



**35%** There are slightly below average scores for Telecoms (25%).

Insurance services, Government and Private hospitals are notably weak on providing information to data subjects

Transparency is an issue for all sectors.



## Summary of scores

Table 2: Summary of scores

	Complies with privacy best practices	Gives information to data subject before collection of data)	Mentions third parties with whom personal data is shared with	Practice Robust Data Security.	How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period	Total
<b>SOCIAL SECURITY</b>	100%	100%	100%	100%	0%	80%
<b>E-COMMERCE</b>	83%	67%	33%	67%	0%	50%
<b>FINANCIAL SERVICES</b>	80%	40%	0%	60%	0%	36%
<b>TELECOM SERVICES</b>	50%	25%	0%	100%	0%	35%
<b>GOVERNMENT AGENCIES</b>	25%	0%	25%	75%	0%	25%
<b>INSURANCE SERVICES</b>	43%	14%	0%	57%	0%	23%
<b>PRIVATE HOSPITAL</b>	0%	0%	0%	0%	0%	0%

## Part 2: A benchmark across other African countries where some of the assessed companies operate.

**In some countries we see a more robust private policy document compared to others.**

An evaluation of the performance of some of the assessed companies across different countries clearly shows a preferential treatment for selective countries. This is evidenced from the noticeable variations in length of privacy policies as well as the number of rights that users are exposed to. This is a case of practicing inconsistencies in exercising private policies.

To augment the argument, further analysis was done on the length of words in the respective policy documents, and we see that the fewer the words, the fewer rights mentioned or not mentioned at all. Questions arise on why the inconsistency in the practice of the assessed companies. Privacy policy documents in countries like Nigeria and South Africa are more robust for most companies compared to others. It can be argued that

the law and the authorities in these countries are strong and working.

Airtel, MTN, Stanbic Bank and Old Mutual have obviously different privacy policies in different African countries

### Different Privacy Policies within the same company

- Jumia and Kikuu has the same privacy policy that covers all its countries.

- Notably, Kikuu's privacy policy is the same with Jumia's

- The policies for both Jumia and KIKUU's policy were seen to be ambiguous about data subject's rights. It seems only in countries with specific laws that users will enjoy certain rights.

## Part 3: Common Apps in Uganda & Technology Analysis

It was common to find trackers in all Apps assessed. **Trackers are defined as a piece of software meant to collect data about you or your usages.** Trackers are known to present different levels of (privacy) intrusion, ranging from crash reporting, analytics, virtual profiling, digital identity, targeted advertising and geographical location of mobile devices.

Some of these apps were seen to be potentially be dangerous, especially those that have location, profiling trackers and those request permission permissions, as they have capabilities to access private user data, could cause fraud transactions or automated clicking activities that further cause data depletion for users. Common countries where these apps come from include USA, South Africa and China

A sample of common Apps cited in this report include;

- Common Apps in Uganda with location trackers : **Glovo, Safeboda, Bolt and Stanbic bank**

- Common Apps in Uganda with profiling trackers included: **Jumia, Safeboda, Bolt, Stanbic bank, Absa Uganda**

Apps such as Jiji.ug, KIKUU, and Airtel are requiring much more permissions and dangerous permissions compared to similar app. The table below quantifies the number of dangerous permissions per App.

Other trackers present them in unsuspecting forms such as VPNs, Phone cleaning, Bible reading, Caller IDs of caller Apps contacts. Its hard for a user to be suspicious of the above to have trackers.

Online Apps	Jiji.ug	Kikuu	Jumia	Kikuubo	Masikini
Permission required	35	31	13	13	13
Dangerous permissions required	10	10	1	7	4
Telecom Apps	Airtel	MTN	Cente Mobile		
Permission required	29	15	18		
Dangerous permissions required	13	5	8		

## Conclusions

It is evident from the results that organisations and companies in Uganda are struggling with data protection compliance. Besides having a robust data security and complying with privacy best practices, all sectors are weak on most data privacy standards.

Non-compliance has privacy-related effects including limiting the control a data subject has over his information once it is transferred, **discrimination and potential abuse** by governments, employers, and others; **criminal fraud** and **identity theft**; and **social and reputational harms**. For example, Poor scores on tests and scans done on websites using SSL server tests security headers tool means that a lot of these websites are susceptible to different attacks e.g. injection attacks.

### 4 Things stand out that could be accelerating the problem of data privacy:

There is no continuous monitoring and scrutiny of the environment against issues of data privacy

Compliance to the Data Protection and Privacy Act, 2019 is still slow and in most cases abused because there is no effective security control, effective monitoring and auditing done, thus providing multiple loopholes.

Countries with stronger data protection laws and independent authorities have companies complying to data protection privacy policies, compared to those with weaker laws.

## Key recommendations

1. Companies or organisation to enable the rights for all users whose personal information is held by them.
2. Oblige to data protection regulations where users have a right to access, rectification, data portability, object, erasure and also restrict use.
3. There is need to ensure that all website operators are familiar with data privacy laws that affect their users.
4. There is need for all sectors to implement and maintain reasonable data security measures.

## Background to the study

Data collection and processing has been a major concern for the information age where a lot of data is being generated and processed by state and non-state actors. Our interconnected world has become even more pervasive, ubiquitous and prominent. As personal data has taken an increasing role in all of our lives and our lives translate ever more into electronic media and data, the questions of who collects that data, what it is used for, who it is shared with and what rights we have over that data are as fundamental to us as any other human right.

In 2019, Uganda enacted the Data Protection and Privacy Act 2019 to regulate the processing of personal data by both public and private entities with the aim of protecting people and their data from various risks that could result into not only infringements of the right to privacy but also other rights such as property rights with varying consequences.

In this era of unprecedented data collection and digital surveillance, the data retained by state agencies, stored on our cell phones, laptops, and especially our online services is a magnet for government and companies to profile us, exert power and make profits.

## About the Scorecard

The Privacy Scorecard is a monitoring tool used to provide Ugandans with critical information on how different data collectors/processors comply with the Data Protection and privacy Act, 2019 as well as the principles and standards of data protection, to empower data subjects to have control over their personal data and make informed choices.

The scorecard focuses on the law, corporate policies and practices. It will turn a spotlight on how the policies of private and public sectors either advance or hinder the privacy rights of users and it will recognize those companies or government agencies that buttress and ensure data protection and privacy best practices. The idea is to protect data privacy rights of individuals by ensuring that data collector/processors bring more

Data collectors/processors are required to be transparent about access to and use of personal data, and to respect our right to privacy and dignity at all times as stipulated in the data protection law. And some companies are increasingly meeting those expectations, but there are still many companies that lag behind, fail to enact best practices around transparency, or don't prioritize user privacy and dignity.

Unwanted Witness has therefore introduced the inaugural Privacy Scorecard that seeks to encourage data collectors/processors adopt data protection best practices, as well as empower citizens in Uganda to demand for information pertaining to how their personal data is collected, what it is used for and who it is disclosed to. At the same time recognise data collectors/processors that have complied with data protection laws and best practices.

This Unwanted witness report details what exactly companies in Uganda are doing – or failing to do – to protect their users from potentially invasive data requests from Government and other 3rd Party players.

transparency and accountability to how they use and divulge people's data.

The role of The Privacy Scorecard is to provide objective measurements for analyzing the policies and practices of major data collectors when it comes to handling data. We focus on a handful of specific, measurable criteria that can act as a vital stopgap against unfettered abuse of user data. Through this scorecard, we hope to galvanize widespread changes in the policies of private and public data collectors to ensure that citizen's digital lives are not subject to manipulation, hence safeguarding human rights and dignity.

# Scorecard criteria

- Only publicly available privacy policy positions can qualify for credits in this Scorecard. Privacy positions, practices, or policies that are conveyed privately or internal corporate standards, regardless of how laudable, are not factored into our decisions to award organizations/companies' credit in any category.
- Requiring public documentation serves several purposes.
  1. First, it ensures that companies cannot secretly change an internal practice in the future to hoodwink customers, but must also change their publicly posted policies—which can be noted and documented.
  2. Second, by asking companies to put their privacy policies and practices in writing, we can examine each policy closely and prompt a larger public conversation about what standards these organisations should strive for.
  3. Third, it helps organisations review one another's policies around law enforcement access, which can serve as a guide for start-ups and others looking for examples of organisations standing up for user privacy.
- In this scorecard, we strive to offer ambitious but practical standards. To that end, we only include criteria that at least one organisation has already adopted. This ensures that we are highlighting existing and achievable best practices, rather than theoretical policies.
- Each year, we review the criteria we used in prior years and make any adjustments that may be necessary to ensure the scorecard is keeping pace with modern technology policy trends. We intend to analyse five criteria for this Scorecard.

## 1. Complies with privacy best practices (An Accessible and Noticeable Privacy Policy)

This is a combined category that measures companies/agencies on two criteria:

The company/agency must have a public, published,

NOTICEABLE, clear and comprehensive Privacy Policy. This helps users make informed choices to assess the privacy and human rights risks they face when using a particular service. Companies must fulfil this criterion in order to earn a star.

## 2. Gives information to data subject before collection of data. (Rights of data subjects as provided by DPPA 2019)

To earn a star in this category, companies/agencies must promise to oblige with Section 13 of the DPPA and inform users clearly at the time of collecting their data about at least:

- Who your company/agency is (your contact details, and those of your DPO if any)
- Why your company/agency will be using their personal data (purposes)
- The nature and category of personal data being collected
- The legal justification for processing their data;
- For how long the data will be kept;
- Who else might receive it;
- That they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection
- Their right to lodge a complaint with a National Information and Technology Authority, Uganda (NITA-U);
- Their right to withdraw consent at any time;

The information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means where appropriate. Your company/organisation must do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge. We allow exceptions for that, to the extent allowed by law.

### 3. Mentions third parties with whom personal data is shared with.

To earn a star, a company/agency must have a public policy that ensures users data is not unlawfully disclosed to third parties as prohibited by Section 35 of DPPA. They should be clear on how they handle user information, so that it's easy to assess the privacy, security, and human rights risks of using their services.

Organizations tend to not sufficiently disclose what user information they share and with whom. This has potential for harm to individuals and to vulnerable communities. Failure to be open with personal data is shared with constitutes a betrayal of user trust and lack of respect for user rights. We allow exceptions for companies/agencies and third parties that, to the extent allowed by law, voluntarily share data with law enforcement or intelligence agencies directly for emergency access, to report crimes where the company or its customers are themselves victims, or to share computer security threat indicators.

### 4. Practice Robust Data Security.

To earn a star in this category, companies/agencies must publicly commit to implement data security measures pursuant to Section 20 of the DPPA. A data is expected to take all steps to safeguard against unauthorised or accidental access, processing or erasure to, alteration,

disclosure or destruction of, personal data and against accidental loss of personal data. Data security and data privacy often go hand-in-hand. Without proper security protocols in place, it's impossible for companies/agencies to guard against threats from outside and within.

All these steps are relevant:

- The place or location where the personal data is stored,
- The security measures incorporated into any equipment in which the personal data are stored,
- The measures taken for ensuring the reliability, integrity and competence of the personnel having access to the personal data,
- The measures taken for ensuring the secure transmission of the personal data.

### 5. Accountability. How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period (A Transparency Report)

The company must have published a transparency report as a sign of being accountable and transparent with users' data as required by Section 3 (a) and (f) of the Data Protection and Privacy Act 2019.

## Score card criteria/Categories

In this scorecard study, sectors below were assessed on how government agencies or companies uphold the data protection standards, and how they instil these standards into products and services to power the data privacy agendas of all those they touch. These varied and included the following:

1. Financial services
2. Insurance services
3. Social security
4. Healthcare
5. Retail/E-commerce
6. Telecoms
7. Government

# Score card criteria/Categories

## 1. Financial Services

Data privacy concerns are particularly paramount for companies in the financial sectors. Banks and other financial institutions manage a large volume of sensitive information about their customers, and the breach of such data can have dire consequences. Workers at banks need certain information to verify the identities of those accessing an account belonging to a client (Know Your Customer).

Customers use their bank cards for transactions trusting that their banking institutions have proper security in place to prevent their information from being stolen. They're also putting confidence in the fact that their institution won't abuse that information by selling it for other purposes without their explicit permission.

The issue of consent gets blurred in this age of digital exchange. Consumers might not realize what rights

they're signing away in a contract or other agreement with a bank or financial institution. They might not fully understand the sensitive nature of the data they're providing, or the consent they're granting when they utilize banking forms, websites or apps. With data-driven innovations such as open banking transforming the customer experience, banks and other financial institutions may struggle with finding the balance between maximizing the customer experience and ensuring adequate security for sensitive personal data. The crux of the matter is that banks need to leverage big data in order to keep pace in today's highly competitive landscape, yet one misstep with sensitive consumer data can have lasting damage on an institution's reputation – and consumer trust.

## 2. Insurance services

The insurance industry has always heavily depended on using large amounts of personal data of policy holders. This data collected, processed and used to handle insurance applications, implement policies and process benefits, to provide advice and assistance. And to assess the risk to be insured, to check the insurer's obligation to perform and to prevent insurance abuse in the interest of the community of policyholders. Today, insurance undertakings are no longer capable to fulfil these tasks without the help of electronic data processing. Ensuring informational self-determination and protection of privacy, as well as the security of data processing, should be the main concerns for the insurance sector in order to ensure the confidence of policyholders.

in order to meet the principles of transparency, of necessity of the data processing operations and of data minimisation.

Maintenance of Insurance Records—insurers are required to ensure that: The system in which the policy and claim records are maintained has adequate security features and maintain total confidentiality of policyholder information unless it is legally necessary to disclose the same to statutory authorities. Consent especially relating to the processing of special personal data can no longer be implied, it must be freely given, and specific, informed, unambiguous, clear affirmative and no imbalance of power must exist.

All provisions on the processing of data have to be in line with the provisions of the DPPA and with all sector-specific regulations on data protection; in addition to that, all insurance undertakings joining this code of conduct are obliged to undertake particular efforts



### 3. Social Security

The implementation of social protection schemes such as NSSF requires collecting variety of information including those identifying beneficiaries and their dependants or carers, earnings, employers, contact details, and more. It is essential that the collection of such information is done without breaching the right to privacy. In this regard, personal information should be kept private and free from misuse, and collected in a lawful manner, only when necessary. This further requires ensuring data is collected with the knowledge and consent of the data subject, is accessible to him or her, and is accurate, complete and up-to-date.

Access to this information should be clearly regulated and sharing of information strictly limited to exchanges necessary for the functioning of the system. Sound measures need to be put in place to ensure the security

of the information stored and to prevent unauthorized access. From a human rights perspective, transparency and access to information are critical safeguards against corruption, and wastage, and increase accountability. Beneficiaries and potential beneficiaries with limited access to information face impediments to their ability to claim their rights. Transparency and access to information should be ensured while guaranteeing the protection of privacy and personal information – based on the DDPA and international standards. Personal information concerning beneficiaries or potential beneficiaries of social protection programmes is highly sensitive, and has the potential to cause stigmatization or other discriminatory practices, or expose beneficiaries to personal security risks.

### 4. Healthcare

Personal data has fundamentally changed the way institutions manage, analyse and leverage data in any industry. One of the most promising fields where personal data can be applied to make a change is healthcare. Personal healthcare data has considerable potential to improve patient outcomes, predict outbreaks of epidemics, gain valuable insights, avoid preventable diseases, reduce the cost of healthcare

delivery and improve the quality of life in general. However, deciding on the allowable uses of data while pre- serving security and patient's right to privacy is a difficult task. Personal healthcare data, no matter how useful for the advancement of medical science and vital to the success of all healthcare institutions, can only be used if security and privacy issues are addressed.

### 5. Retail/ E-commerce

Privacy and security threats in E-commerce has become a discussion topic among the users; their users are not reluctant from the pain of data privacy issues and threats of security. If these privacy and security threats are not eliminated, users never trust, visit or shop at an

E-commerce site. Maintenance of users' privacy online is one of the concerns of E-commerce. The usage of technical methods to capture their user's data has been raising the privacy issues.

## 6. Telecom

The telecommunication environment in Uganda as a digital ecosystem involves multiple entities such as Devices, Telecom Service Providers (TSPs), Communication Networks Browsers, Operating Systems, Applications, Over the Top (OTT) service providers, etc. These entities routinely access, collect and assemble data pertaining to the user. Such data

could include personal information, in which case, a user's privacy is likely to be infringed and should be with the informed and explicit consent of users. It is therefore incumbent upon telecom companies to secure the data privacy interests of telecommunication users.

## 7. Government Agencies

Data security means protecting data from destruction and any unwanted or unauthorized actions through the implementation of appropriate technical and organizational measures.

Government agencies engaged in the processing of personal data are obligated to:

- Through its head of agency, designate a Data Protection Officer;
- Conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data;
- Create privacy and data protection policies;
- Conduct an annual mandatory, agency-wide training on privacy and data protection policies, and a similar training during all agency personnel orientations.

In this scorecard study, sectors below were assessed on how government agencies or companies uphold the data protection standards, and how they instil these standards into products and services to power the data privacy agendas of all those they touch. These varied and included the following

- Financial services
- Insurance services
- Private hospitals
- Telecoms
- Social security
- Government
- E-commerce

Unwanted witness rated all of the companies on a two-star scale, for either cross or star, across five different measures as below:

- Complies with privacy best practices
- Giving information to data subject before collection of data)
- Mentioning third parties with whom personal data is shared with
- Practice Robust Data Security.
- Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period

The rating system had a star, which means that a company complied and rates (1), and a cross for non-compliance rated as zero(0). The star meant that the companies are less likely to sell you out, while the cross meant no effort to protect users from government and 3rd part requests.

<p><b>Complies with privacy best practices</b></p> <p>This is a combined category that measures companies/agencies on two criteria:</p> <ol style="list-style-type: none"> <li>1. The company/ agency must have a public, published, NOTICEABLE, clear and comprehensive Privacy Policy. This helps users make informed choices to assess the privacy and human rights risks they face when using a particular service.</li> <li>2. Companies must fulfil this criterion in order to earn a star.</li> </ol>	<p><b>Gives information to data subject before collection of data)</b></p> <p>To earn a star in this category, companies/agencies must promise to oblige with Section 13 of the DPPA and inform users clearly at the time of collecting their data about at least:</p> <ul style="list-style-type: none"> <li>• Who your company/ agency is (your contact details, and those of your DPO if any)</li> <li>• Why your company/ agency will be using their personal data (purposes)</li> <li>• The nature and category of personal data being collected</li> <li>• The legal justification for processing their data;</li> <li>• For how long the data will be kept;</li> <li>• Who else might receive it;</li> </ul> <p>That they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection</p> <p>Their right to lodge a complaint with a National Information and Technology Authority, Uganda (NITA-U);</p> <p>Their right to withdraw consent at any time;</p> <p>The information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means where appropriate. Your company/ organisation must do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge. We allow exceptions for that, to the extent allowed by law.</p>	<p><b>Mentions third parties with whom personal data is shared with</b></p> <p>To earn a star, a company/agency must have a public policy that ensures users data is not unlawfully disclosed to third parties as prohibited by Section 35 of DPPA. They should be clear on how they handle user information, so that it's easy to assess the privacy, security, and human rights risks of using their services.</p> <p>Organizations tend to not sufficiently disclose what user information they share and with whom. This has potential for harm to individuals and to vulnerable communities. Failure to be open with personal data is shared with constitutes a betrayal of user trust and lack of respect for user rights.</p> <p>We allow exceptions for companies/ agencies and third parties that, to the extent allowed by law, voluntarily share data with law enforcement or intelligence agencies directly for emergency access, to report crimes where the company or its customers are themselves victims, or to share computer security threat indicators.</p>	<p><b>Practice Robust Data Security</b></p> <p>To earn a star in this category, companies/ agencies must publicly commit to implement data security measures pursuant to Section 20 of the DPPA. A data is expected to take all steps to safeguard against unauthorised or accidental access, processing or erasure to, alteration, disclosure or destruction of, personal data and against accidental loss of personal data.</p> <p>Data security and data privacy often go hand-in-hand. Without proper security protocols in place, it's impossible for companies/agencies to guard against threats from outside and within.</p> <p>All these steps are relevant:</p> <ul style="list-style-type: none"> <li>• The place or location where the personal data is stored,</li> <li>• The security measures incorporated into any equipment in which the personal data are stored,</li> <li>• The measures taken for ensuring the reliability, integrity and competence of the personnel having access to the personal data,</li> <li>• The measures taken for ensuring the secure transmission of the personal data.</li> </ul>	<p><b>Accountability</b> <b>How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period</b></p> <p>The company must have published a transparency report as a sign of being accountable and transparent with users' data as required by Section 3 (a)and (f) of the Data Protection and Privacy Act 2019.</p>
--	--	--	--	---

# Complete Findings

This is a three part report, that includes:

- **Part 1:** Privacy scorecard performance – Uganda performance (How big companies in Uganda are complying with the privacy law
- they operate - How they comply with the privacy law in other countries.
- **Part 2:** A benchmark across other market where
- **Part 3:** Most used apps in Uganda

## Part 1: Privacy scorecard performance – Uganda performance (How big companies in Uganda are complying with the privacy law.

In this section, we provide the detailed findings of the research section that provides figures on how;

- Companies comply to the privacy laws.
- Index score



PRIVACY SCORECARD		e-commerce						Total score	% Score
Parameters		Safeboda	Jumia	Kikuubo online	Masikini	Kikuu	Glovo		
1	Complies with privacy best practices (An Accessible and Noticeable Privacy Policy)	1	1	1	1	1	0	5	83%
2	Gives information to data subject before collection of data.(Rights of data subjects as provided by DPPA 2019)	1	1	1	0	1	0	4	67%
3	Mentions third parties with whom personal data is shared with	1	0	1	0	0	0	2	33%
4	Practice Robust Data Security.	0	1	0	1	1	1	4	67%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period (A Transparency Report.)	0	0	0	0	0	0	0	0%
								<b>Av. score</b>	<b>50%</b>
<b>Total score</b>		<b>3</b>	<b>3</b>	<b>3</b>	<b>2</b>	<b>3</b>	<b>1</b>	<b>Av. Score</b>	
<b>% SCORE</b>		<b>60%</b>	<b>60%</b>	<b>60%</b>	<b>40%</b>	<b>60%</b>	<b>20%</b>	<b>50%</b>	

- The report gives e-commerce a perfect rating of 50%.
- E-commerce companies performed best on compliance with privacy best practices (83%), and had relatively good scores for a robust data security and providing info to data subjects and lowest for government data requests, with 5 out of 6 rating for compliance.
- A range of companies i.e. Safeboda, Jumia, Kikuubo online and Kikuu perform relatively better. Glovo and Masikini recorded the lowest performance.

# E-commerce Performance summary

Most companies under e-commerce complied with privacy best practices by having a noticeable and accessible policy especially placed at the footer of their websites.

They also disclose the rights of the data subjects as provided by DPPA 2019. Common practices include;

- the right to access, correct or erase your personal data, object to or restrict processing of user’s personal data, and unsubscribe from their emails and newsletters
- The right to be informed about our collection and use of personal data.
- The right to access the personal data they hold about users.
- The right to have users’ personal data rectified if any of user’s personal data held by them is inaccurate or incomplete.
- The right to be forgotten.

- The right to restrict the processing of your personal data.
- The right to object us from using your personal data for particular purposes
- The right to data portability.
- The right to withdraw consent.
- Rights relating to automated decision making

With the exception of Safeboda that mentions third parties with whom users’ personal data is shared with e.g. Wiz Rocket trading as CleverTap based in the USA and Kikuubo Online which mentions Lotus Private Cloud and through OVH Cloud in Canada & USA which handle all storage processing handled, and Pegasus Technologies Ltd based in Uganda that handles all its transaction processing, all other players have no mention of third parties with whom personal data is shared with.

# E-commerce Performance indicators

On having a robust data security, some of these e-commerce players show vulnerabilities to attack. For example;

Some of them do not have SSL certificates

Their scores on the SSL lab, as well as security headers are comparatively low

In the area of accountability and transparency, we see no information available to the effect that there is information that is shared with 3rd parties such as government and law enforcement agencies.

## Index score



PRIVACY SCORECARD		Social security		% Score
Parameters	NSSF	Total score	Av. score	
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	1	1	100%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	1	1	100%
3	Mentions third parties with whom personal data is shared with	1	1	100%
4	Practice Robust Data Security.	1	1	100%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0%
<b>Total score</b>		<b>4</b>	<b>4</b>	<b>80%</b>
<b>% SCORE</b>		<b>80%</b>	<b>80%</b>	

- The report gives Social security a rating of 80%.
- NSSF performed exceptionally well on all metrics except for accountability.

**SOCIAL SECURITY**

80%

PRIVACY SCORECARD		Social security		
Parameters		NSSF	Total score	% Score
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	1	1	100%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	1	1	100%
3	Mentions third parties with whom personal data is shared with	1	1	100%
4	Practice Robust Data Security.	1	1	100%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0%
<b>Total score</b>		<b>4</b>	<b>Av. score</b>	<b>80%</b>
<b>% SCORE</b>		<b>80%</b>	<b>Av. Score</b>	<b>80%</b>

- The report gives Social security a rating of 80%.
- NSSF performed exceptionally well on all metrics except for accountability.

**FINANCIAL SERVICES**

36%

PRIVACY SCORECARD		Financial Services					Total score	% Score
Parameters		Stanbic Bank	Stanchart	Centenary Bank	Absa	DFCU		
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	1	1	0	1	1	4	80%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	0	1	0	1		2	40%
3	Mentions third parties with whom personal data is shared with	0	0	0	0	0	0	0%
4	Practice Robust Data Security.	1	1	0	1	0	3	60%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0	0	0	0	0%
<b>Total score</b>		<b>2</b>	<b>3</b>	<b>0</b>	<b>3</b>	<b>1</b>	<b>Av. score</b>	<b>36%</b>
<b>% SCORE</b>		<b>40%</b>	<b>60%</b>	<b>0%</b>	<b>60%</b>	<b>20%</b>	<b>Av. Score</b>	<b>36%</b>

- The report gives financial services a rating of 36%.
- Financial service companies performed best on compliance with privacy best practices (80%), and relatively better on robust data security and poorest on 3rd party mentions as well as on data accountability.
- A range of companies i.e.. Absa and Stanchart perform relatively better. DFCU and Centenary Bank recorded the lowest performance.

# Financial services Performance summary

With the exception of Centenary bank, all other commercial banks assessed have a noticeable and accessible privacy policy located at the footer of its website.

Most have a robust data security. Their SSL server scores are good and strong indication of security headers. Centenary and DFCU are noticeably weak, with no existence of security headers, poor SSL server scores, have Facebook trackers and DFCU in particular being prone to key logging.

On whether banks give information to data subject before collection of data, this is not consistent across banks. While a few of them do, others do not. For example;

- Standard Chartered Bank discloses users' rights which include; the right to request access to personal information, the right to have it corrected where appropriate, and the right delete any of your personal data held by the bank, and Absa Bank makes mention of the user's rights which include; the right to access your personal information, the right to ask Absa to correct any

of your personal information that is incorrect, the right to destroy your personal information, and the right to processing your personal information.

- Both Stanbic Bank and DFCU does not disclose all the rights needed to the data subject as required by the DPPA 2019, with the exception of DFCU Bank does not disclose all the rights needed to the data subject as required by the DPPA 2019. It only mentions two rights i.e., User's right to object to certain types of processing and the right to query a decision that we make about a product or service that users have applied for and that was made solely by automated means.
- Others such as Centenary bank has no information available to the effect.

All banks do not make mention of any third parties with whom users' information is shared with.

## TELECOMS

35%

### PRIVACY SCORECARD

Parameters		Telecoms				Total score	% Score
		MTN	Airtel	UTL	Africell		
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	0	1	0	1	2	50%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	0	0	0	0	0	0%
3	Mentions third parties with whom personal data is shared with	0	0	0	0	0	0%
4	Practice Robust Data Security.	1	1	1	1	4	100%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0	0	0	0%
						<b>Av. score</b>	<b>35%</b>
<b>Total score</b>		<b>1</b>	<b>2</b>	<b>1</b>	<b>3</b>	<b>Av. Score</b>	
<b>% SCORE</b>		<b>20%</b>	<b>40%</b>	<b>20%</b>	<b>40%</b>	<b>35%</b>	

- The report gives Telecom services a rating (35%) in its privacy score card report, which rates companies on their efforts to secure consumer data against government and 3rd party snooping.
- Telecom companies performed best on practicing robust

data security (100%) and relatively better on compliance with privacy best practices (50%) and poorest on 3rd party mentions as well as on data accountability.

- Besides Africell and Airtel, the rest of the Telecoms have very low performance.

# Telecom services Performance summary

Telecom players perform best on practicing Robust Data Security. Their SSL server of the website scored well, and with a B capping being the worst performance. The only vulnerability being for MTN and Airtel having trackers belonging to Twitter, Facebook, LinkedIn and Google.

Telecoms record poor results against all other criteria. For example

- there is no noticeable and Accessible Privacy

Policy on either of the players.

- their Privacy Policies do not disclose any user rights, with the exception of MTN that mentions the right to access to user information and the right to correct user information.
- Do not mention of any third parties with whom users information is shared with.

## INSURANCE SERVICES

23%

PRIVACY SCORECARD		Insurance services							Total score	% Score
Parameters		UAP	SANLAM	BRITAM	GOLDSTAR	JUBILEE	SWICO	ICEA		
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	1	0	1	0	0	1	0	3	43%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	0	0	0	0	0	0	1	1	14%
3	Mentions third parties with whom personal data is shared with	0	0	0	0	0	0	0	0	0%
4	Practice Robust Data Security.	1	0	1	1	0	0	1	4	57%
5	How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0	0	0	0	0	0	0%
									<b>Av. score</b>	<b>23%</b>
<b>Total score</b>		<b>2</b>	<b>0</b>	<b>2</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>Av. Score</b>	
<b>% SCORE</b>		<b>40%</b>	<b>0%</b>	<b>40%</b>	<b>20%</b>	<b>0%</b>	<b>20%</b>	<b>40%</b>	<b>23%</b>	

- The report gives Insurance services below average rating (23%) in its privacy score card report, which rates companies on their efforts to secure consumer data against government and 3rd party snooping.
- Insurance services performed relatively well on practicing robust data security (57%) and compliance with best practices (43%), with miserably low scores on the rest of the privacy

metrics.

- Only BRITAM,UAP and ICEA scored better (40%) with at least 2 out of 5 scoring. All other insurance companies' scores were miserably low.
- SANLAM and JUBILEE registered the poorest performance overall.

# Insurance services Performance summary

UAP, Britam and Statewide have noticeable and accessible privacy policy located at the footer of its website. Though called "Privacy Notice". While ICEA has a private policy, its not noticeable.

On robust data security, a few of the player websites reported a good score on their SSL servers tests and employ the necessary security headers. However, some had Facebook trackers, thus showing some level of vulnerabilities. Majority of them reported very poor scores.

Only ICEA discloses to data subjects the following rights;

- Access your personal data by making a subject access request,
- Rectification, erasure or restriction of your information where this is justified,
- Object to the processing of your information where this is justified and
- Data portability

All insurance players do not mention of any third parties with whom users information is shared with



**GOVERNMENT AGENCIES** 25%

PRIVACY SCORECARD		Government				Total score	% Score
Parameters		URA	NIRA	MOW&T	Directorate of citizenship		
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	0	0	1	0	1	25%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	0	0	0	0	0	0%
3	Mentions third parties with whom personal data is shared with	0	0	0	0	0	0%
4	Practice Robust Data Security.	0	1	1	1	3	75%
5	How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0	0	0	0%
						<b>Av. score</b>	<b>25%</b>
<b>Total score</b>		<b>0</b>	<b>1</b>	<b>2</b>	<b>1</b>	<b>Av. Score</b>	
<b>% SCORE</b>		<b>0%</b>	<b>20%</b>	<b>40%</b>	<b>20%</b>	<b>25%</b>	

- The report gives Government a below average rating (25%) in its privacy score card report, which rates companies on their efforts to secure consumer data against government and 3rd party snooping.
- Government performed best on practicing robust data security (75%). And scores miserably low on the rest of the privacy metrics.
- Only Ministry of works and transport(MOW&T) scored better with two scores out of the 5, the rest of Government had very low or no score performance. URA registered the poorest performance overall.

## Government agencies Performance summary

Government agencies perform well on practicing Robust Data Security. However, while they score relatively well on the SSL server tests on the website, most of them were said to lack security headers. Others like URA were found to have multiple trackers belonging to Facebook, Alphabet and other third-parties.

Besides Ministry of Works and Transport, all other government agencies had no Noticeable and Accessible privacy policy on the footer of its website, like it's a common practice.

Government agencies score poorly on all other measures.

**PRIVATE HOSPITALS** 0%

PRIVACY SCORECARD Parameters		Private Hospital					Total	%score
		Case	IHK	Kampala Hospital	Nakasero	Paragon		
1	Complies with privacy best practices ( <b>An Accessible and Noticeable Privacy Policy</b> )	0	0	0	0	0	0	0%
2	Gives information to data subject before collection of data.( <b>Rights of data subjects as provided by DPPA 2019</b> )	0	0	0	0	0	0	0%
3	Mentions third parties with whom personal data is shared with	0	0	0	0	0	0	0%
4	Practice Robust Data Security.	0	0	0	0	0	0	0%
5	Accountability How much data was requested and shared with third parties such as government bodies and law enforcement agencies during the assessed period ( <b>A Transparency Report.</b> )	0	0	0	0	0	0	0%
<b>Av. score</b>							0	0%
<b>Av. Score</b>							0	0%
<b>Total score</b>		0	0	0	0	0	0	0%
<b>% SCORE</b>		0%	0%	0%	0%	0%	0%	0%

- The report gives private hospitals a zero(0%) in its privacy score card report, which rates companies on their efforts to secure consumer data against government and 3rd party snooping.
- Private hospitals did not perform on any privacy score card metrics.
- All hospitals investigated returned no results at all.

## Complete Findings

### Part 2: A benchmark across other market where companies operate - How they comply with the privacy law in other countries.

#### Countries measured

The table below provides details of the companies measured in their respective countries.

Company Measured	
Note: Below are the companies we used for the privacy policy analysis	
company	country
Stanbic Bank	South Africa
old mutual	South Africa
MTN	South Africa
Jumia	Nigeria
Airtel	Indian
Kikuu	China
tiktok	China
snapchat	US

#### Privacy rights

Seven (7) Privacy rights were considered. These are the 7 globally accepted and used rights. Below is a list of the rights that were considered in the privacy policy

Rights Considered	
Note: The below rights are taken into consideration when counting number of rights in the privacy policy	
Rights	count
access	1
update,correct	1
delete,erase,cancel	1
restrict data processing, object data processing	1
opt out of marketing, not be the subject	1
withdraw consent	1
query, report, complaint	1

Scoring Scheme		
An evaluation was done on the privacy policies based on the variables above.		
Criteria	Score	Score_group
Mentions 0 Rights	0	right_score
Mentions 1-2 Rights	1	right_score
Mentions 3-4 Rights	2	right_score
Mentions 5+ Rights	3	right_score
Have a noticeable privacy policy	2	notice_score
Have a Privacy Policy through search	1	notice_score
Don't have a privacy policy	0	notice_score
Mentions third parties to whom the data is shared with	1	share_score
doesn't mention third parties with whom the data is shared	0	share_score

## Privacy rights - Scoring scheme

Note: Privacy Policies are measured using three criterias, whether there is a noticeable privacy policy (notice score), how many rights of the data subjects (rights score) and where mention the third parties whom the data is shared with (share score). The total score of the privacy policy is a sum of these three scores

### NCSI Personal Data Protection Index of Countries involved in the measurement

**Note:** The index measures Protection of personal data from the below two perspectives. The score is from 0-4.

- personal data protection legislation
- personal data protection authority

More information can be found at <https://ncsi.ega.ee/>

country	PDP Score
Benin	4
Nigeria	4
Kenya	4
Mauritius	4
Ghana	4
Cote d'Ivoire	4
South Africa	4
Morocco	4
Botswana	4
Chad	4
Madagascar	4
Seychelles	4
Angola	4
Uganda	1
Zambia	1
Cameroon	1
Malawi	1
Liberia	1
Zimbabwe	1
Mozambique	1
Egypt	0
Rwanda	0
Tanzania	0
Sudan	0
Namibia	0
Congo (Democratic Republic of Congo)	0
South Sudan	0

NCSI Index – NCSI personal data protection score for all African countries

More information can be found at <https://ncsi.ega.eg/>.

**Countries ranking with mean scores**

- NCSI index is national cyber security index.
- The sub-indicator used is Protection of personal data.
- The score was determined from 0-4.
- The protection of personal data is evaluated from two perspectives:

personal data protection legislation

personal data protection authority

**Privacy Policy Evaluating Methodology**

Measured the privacy policy in the below two ways.

Whether there is a noticeable privacy policy. There are the three below conditions

There is a noticeable privacy policy.

There is a privacy policy. It's not noticeable but I found it through website search.

There isn't a privacy policy.

# rank	Country	# Number of companies	# Mean Score	NCSI score
1	South Africa	3	6	4
2	Nigeria	4	5.8	4
3	Ghana	4	4	4
3	Kenya	3	4	4
3	Rwanda	3	4	0 (should be updated as 1 as their data protection law came out 2021)
3	Tanzania	3	4	0
7	Botswana	3	3	4
7	Uganda	4	3	1
9	Eswatini	3	2.7	NA
10	Malawi	3	2.3	1
11	Namibia	3	2	0
12	Zambia	3	2	1

## Country Insights

Using the NCSI index, we observe that countries with a data protection legislation and independent data protection authority register more compliance from companies.

These countries include South Africa and Nigeria. Companies with weaker protection laws such as such as Zambia, Namibia, Malawi have companies exposing

compromised privacy policies.

Uganda ranks 7 among 12 countries.

Countries with data protection legislation and data protection authority tend to have better privacy policies. However, Botswana is an exception.

# Stanbic Bank

Stanbic Bank privacy policy is inconsistent across countries. An analysis of the policy shows that the length of their privacy policies varies from one country to another. Evidently, the longer the policy, the more robust and representative it is. Countries that have a more robust policy, also have full content in respect to rights. South

Africa, Mauritius, Nigeria are examples.

In Uganda, the document depicts only 4 out of the 7 rights.

Mozambique, Zambia, Botswana and Malawi have the least robust policies, and no single right appears in the document.

**NOTE:** Only includes companies with obvious variations of privacy policies among African countries.

Company	Country	Policy length	Noticeable	Rights no	Share	Length group	Right group	protection_personal_data_ncsi	share_score	right_score	notice_score	total
Stanbic Bank	South Africa	6097	Y	7	Y	>4000	5+	4	1	3	2	6
Stanbic Bank	Mauritius	4119	Y	5	Y	>4000	5+	4	1	3	2	6
Stanbic Bank	Nigeria	1628	Y	6	M	1000-2000	5+	4	0	3	2	5
Stanbic Bank	DRC	1611	Y	4	M	1000-2000	3~4	0	0	2	2	4
Stanbic Bank	Tanzania	1508	Y	4	M	1000-2000	3~4	0	0	2	2	4
Stanbic Bank	Namibia	1414	Y	4	M	1000-2000	3~4	0	0	2	2	4
Stanbic Bank	Lesotho	1375	Y	4	M	1000-2000	3~4	0	0	2	2	4
Stanbic Bank	Uganda	1358	Y	4	M	1000-2000	3~4	1	0	2	2	4
Stanbic Bank	Kenya	1346	Y	4	M	1000-2000	3~4	4	0	2	2	4
Stanbic Bank	Zimbabwe	1338	Y	4	M	1000-2000	3~4	1	0	2	2	4
Stanbic Bank	Cote d'Ivoire	1324	Y	4	M	1000-2000	3~4	4	0	2	2	4
Stanbic Bank	Eswatini	1320	Y	4	M	1000-2000	3~4	0	0	2	2	4
Stanbic Bank	Ghana	1299	Y	4	M	1000-2000	3~4	4	0	2	2	4
Stanbic Bank	Angola	1494	Y	1	M	1000-2000	1~2	4	0	1	2	3
Stanbic Bank	Mozambique	1540	Y	0	M	1000-2000	0	1	0	0	2	2
Stanbic Bank	Malawi	813	Y	0	M	500-1000	0	1	0	0	2	2
Stanbic Bank	Botswana	712	Y	0	M	500-1000	0	4	0	0	2	2
Stanbic Bank	Zambia	0	N	0	N	<500	0	1	0	0	0	0

# Old Mutual

Like Stanbic, the Old Mutual privacy policy is also inconsistent. An analysis of the policy shows that the length of their policies varies from one country to another. Evidently, the longer the policy, the more robust and representative it is. Countries that have a more robust policy, also have full content in respect to

rights. Nigeria, Kenya, South Africa are examples.

In Uganda, the document has no single right, and is listed as one of the countries with the least robust policies, the other being Namibia.

**Comparison of privacy policy of selected companies among African countries**

**Note:** Only includes companies with obvious variations of privacy policies among African countries.

Company	Country	Policy Length	Noticable	Rights No	Share	Length Group	Right Group	Protection Personal Data NCSI	Share Score	Right Score	Notice Score	Total
Old Mutual	Nigeria	3726	Y	7	Y	2000-4000	5+	4	1	3	2	6
Old Mutual	Kenya	3352	Y	5	Y	2000-4000	5+	4	1	3	2	6
Old Mutual	South Africa	1853	Y	5	Y	1000-2000	5+	4	1	3	2	6
Old Mutual	Zimbabwe	1706	Y	5	Y	1000-2000	5+	1	1	3	2	6
Old Mutual	Ghana	1692	Y	5	Y	1000-2000	5+	4	1	3	2	6
Old Mutual	Rwanda	1623	Y	5	Y	1000-2000	5+	0	1	3	2	6
Old Mutual	Tanzania	1537	Y	5	Y	1000-2000	5+	0	1	3	2	6
Old Mutual	South Sudan	1635	Y	4	Y	1000-2000	3~4	0	1	2	2	5
Old Mutual	Eswatini	1577	Y	1	M	1000-2000	1~2	0	0	1	2	3
Old Mutual	Botswana	318	Y	1	M	<500	1~2	4	0	1	2	3
Old Mutual	Malawi	318	Y	1	M	<500	1~2	1	0	1	2	3
Old Mutual	Uganda	1612	Y	0	N	1000-2000	0	1	0	0	2	2
Old Mutual	Namibia	402	Y	0	M	<500	0	0	0	0	2	2

## Old Mutual

MTN is equally selective. Their privacy policy is also inconsistent. An analysis of the policy shows that the length of their policies varies from one country to another. Evidently, the longer the policy, the more robust and representative it is. Countries that have a more robust policy, also have full content in respect to rights. Nigeria,

Zambia, South Africa are examples.

In Uganda, the document has documented 2 rights.

Countries like Cameroon, Liberia, Sudan, South Sudan and Namibia have no single policy document.

Comparison of privacy policy of selected companies among African countries												
Note: Only includes companies with obvious variations of privacy policies among African countries.												
Company	Country	Policy Length	Noticeable	Rights No	Share	Length Group	Right Group	Protection Personal Data NCSI	Share Score	Right Score	Notice Score	Total
MTN	South Africa	3749	Y	6	Y	2000-4000	5+	4	1	3	2	6
MTN	Nigeria	2733	Y	5	Y	2000-4000	5+	4	1	3	2	6
MTN	Zambia	2255	Y	6	Y	2000-4000	5+	1	1	3	2	6
MTN	Cote d'Ivoire	1685	Y	5	Y	1000-2000	5+	4	1	3	2	6
MTN	Ghana	1083	M	3	Y	1000-2000	3-4	4	1	2	1	4
MTN	Botswana	1903	Y	2	Y	1000-2000	1-2	4	1	1	2	4
MTN	Rwanda	1103	Y	2	Y	1000-2000	1-2	0	1	1	2	4
MTN	Republic of Congo	1021	Y	2	Y	1000-2000	1-2		1	1	2	4
MTN	Uganda	978	Y	2	Y	500-1000	1-2	1	1	1	2	4
MTN	Guinea	547	M	4	N	500-1000	3-4		0	2	1	3
MTN	Eswatini	411	M	0	Y	<500	0		2	0	0	2
MTN	Benin	1291	Y	4	N	1000-2000	3-4	4	2	2	0	4
MTN	Cameroon	0	N	0	N	<500	0	1	0	0	0	0
MTN	Liberia	0	N	0	N	<500	0	1	0	0	0	0
MTN	Sudan	0	N	0	N	<500	0	0	0	0	0	0
MTN	South Sudan	0	N	0	N	<500	0	0	0	0	0	0
MTN	Namibia	0	N	0	N	<500	0	0	0	0	0	0

## Airtel

Airtel has one of the worst privacy policy practices across the countries where it operate. Its privacy policy is equally inconsistent. An analysis of the policy shows that the length of their policies varies from one country to another. Evidently, the longer the policy, the more robust and representative it is.

Only in countries like Nigeria and India does Airtel show rights in its policy document. Majority of the countries have little content in their policies and no right is mentioned in the policy document. Uganda is a victim of this practice.

Comparison of privacy policy of selected companies among African countries												
Note: Only includes companies with obvious variations of privacy policies among African countries												
Company	Country	Policy Length	Noticable	Rights No	Share	Length Group	Right Group	Protection Personal Data NCSI	Share Score	Right Score	Notice Score	Total
Airtel	Nigeria	5269	Y	7	Y	>4000	5+	4	1	3	2	6
Airtel	India	1695	Y	3	Y	1000-2000	3-4	0	1	2	2	5
Airtel	Kenya	618	Y	0	N	500-1000	0	4	0	0	2	2
Airtel	Uganda	573	Y	0	N	500-1000	0	1	0	0	2	2
Airtel	Rwanda	573	Y	0	N	500-1000	0	0	0	0	2	2
Airtel	Tanzania	572	Y	0	N	500-1000	0	0	0	0	2	2
Airtel	Seychelles	571	Y	0	N	500-1000	0	4	0	0	2	2
Airtel	Malawi	565	Y	0	N	500-1000	0	1	0	0	2	2
Airtel	Chad	553	Y	0	N	500-1000	0	4	0	0	2	2
Airtel	Ghana	487	Y	0	N	<500	0	4	0	0	2	2
Airtel	Zambia	703	N	0	N	500-1000	0	1	0	0	0	0
Airtel	DRC	84	N	0	N	<500	0	0	0	0	0	0
Airtel	Niger	82	N	0	N	<500	0	0	0	0	0	0
Airtel	Republic of Congo	81	N	0	N	<500	0		0	0	0	0
Airtel	Madagascar	73	N	0	N	<500	0	4	0	0	0	0
Airtel	Gabon	71	N	0	N	<500	0		0	0	0	0

## Jumia and Kikuu

The two have similar content in their privacy policy that covers all its countries. However Jumia and Kikuu's policy is ambiguous about data subject's rights. It seems only in countries with specific laws that users will enjoy certain rights.

Comparison of privacy policy of selected companies among African countries

**Note:** Only includes companies with no obvious variations of privacy policies among African countries.

Company	Country	Policy Length	Noticable	Rights No	Share	Length Group	Right Group	Share Score	Right Score	Notice Score
Jumia	Cameroon	2255	Y	ambiguous	Y	2000-4000		2		2
Jumia	Kenya	1008	Y	ambiguous	Y	1000-2000		2		2
Jumia	Morocco	992	Y	ambiguous	Y	500-1000		2		2
Jumia	Egypt	974	Y	ambiguous	Y	500-1000		2		2
Jumia	Nigeria	960	Y	ambiguous	Y	500-1000		2		2
Jumia	Cote d'Ivoire	941	Y	ambiguous	Y	500-1000		2		2
Jumia	South Africa	931	Y	ambiguous	Y	500-1000		2		2
Jumia	Uganda	906	Y	ambiguous	Y	500-1000		2		2
KiKUU	Ethiopia	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Tanzania	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Uganda	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Ghana	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Nigeria	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Cameroon	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	DRC	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Congo	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Cote d'Ivoire	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Senegal	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Rwanda	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Kenya	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Zambia	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	Mali	927	Y	ambiguous	Y	500-1000		2		2
KiKUU	South Africa	927	Y	ambiguous	Y	500-1000		2		2

## International Social Media Companies - Companies analysed: Snapchat and Tiktok

### Snapchat

Snapchat has a privacy policy for all countries, all users enjoy 5 rights.

Snapchat has specific terms for Brazil, EEA/UK, California and Mexico that give users more rights.

Tiktok & Snapchat Privacy Policies Analysis								
Company	Country	Length	Noticable	Rights	Share	Length Group	Right Group	
Tiktok	EEA,UK,Switzerland	4941	Y	6	Y	>4000	>5	
Tiktok	Philippines			6	Y		>5	
Tiktok	Brazil			6	Y		>5	
Tiktok	Mexico			5	Y		>5	
Tiktok	Turkey			3	Y		3~4	
Tiktok	South Korea			4	Y		3~4	
Tiktok	Indonesia			3	Y		3~4	
Tiktok	US	3758	Y	2	Y	2000-4000	0-2	
Tiktok	Other Regions	3798	Y	0~2	Y	2000-4000	0-2	
Snapchat	all	3263	Y	5	Y	2000-4000	>5	
Snapchat	Mexico			6	Y		>5	
Snapchat	Brazil			7	Y		>5	
Snapchat	EEA,UK			7	Y		>5	
Snapchat	California			5	Y		>5	

# Tiktok

Tiktok has three different privacy policy that applies to US, EEA/UK/Switzerland, and other Regions

It has country specific terms about user rights for Philippines, Brazil, Mexico, Turkey, South Korea, Indonesia. Users in these countries & in the EEA/UK/Switzerland region enjoy more rights compared to users from other areas.

In the tiktok privacy policy for Other regions, the general user rights are very ambiguous. It seems only in countries with specific laws that users will enjoy certain rights.

One can access and edit most of your profile information by signing into TikTok. You can delete the User Content you uploaded. We also provide a number of tools in Settings that allow you to control, among others, who can view your videos, send you messages, or post comments to your videos. Should you choose to do so, you may delete your entire account in Settings. You may also be afforded rights in your country under applicable laws such as the ability to access your data, delete your data, and potentially others.

## Best practices

Country	Company	Length of privacy policy	Rights terms in the privacy policy
Nigeria Uganda	Safeboda	around 2500	As a data subject, you have the following rights, which we will always work to uphold:  The right to be informed about our collection and use of your personal data. This Privacy Policy should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 14. The right to <b>access the personal data we hold about you</b> . Part 12 will tell you how to do this. The right to have your <b>personal data rectified if any of your personal data held by us is inaccurate or incomplete</b> . Please contact us using the details in Part 14 to find out more. The right to be forgotten. I.e., the right to ask us to <b>delete or otherwise dispose of any of your personal data that we have</b> . Please contact us using the details in Part 14 to find out more. The right to <b>restrict (i.e., prevent) the processing of your personal data</b> . The right to <b>object to us using your personal data for a particular purpose(s)</b> . The right to <b>data portability</b> . This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.
Kenya	Safeboda	8000	The Data Protection and Privacy Act sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details): 3.1 The right to <b>be informed</b> (Part 12); 3.2 The right of <b>access</b> (Part 13); 3.3 The right to <b>rectification</b> (Part 14); 3.4 The right to <b>erasure (also known as the 'right to be forgotten')</b> (Part 15); 3.5 The right to <b>restrict processing</b> (Part 16); 3.6 The right to <b>data portability</b> (Part 17); 3.7 The right to object (Part 18); and 3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

Safeboda presents one of the best practices for consistency across countries where they operate. In all these countries; Uganda, Nigeria and Kenya, the Safeboda private policy is consistent with an exposure of all its rights to users.



## Complete Findings

# Part 3 – TECH ANALYSIS and exploring the most used & Top apps in Uganda.

### ACRONYMS

SSL	Secure Sockets Layer
TLS	Transport Layer Security
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure Hyper-Text Transfer Protocol

## Tools Used.

### Exodus Privacy:

Exodus analyses Android applications. It looks for embedded trackers and lists them. A tracker is a piece of software meant to collect data about you or what you do. In a way, exodus reports are a way of knowing what really the ingredients of the cake you are eating.

Website: <https://reports.exodus-privacy.eu.org/en/>

### Qualys SSL Labs

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet.

Website: <https://www.ssllabs.com/ssltest/>

### Blacklight

This is a real-time website inspector that scans websites and reveals the specific user-tracking technologies on the site.

Website: <https://themarkup.org/blacklight/>

### MyIp.ms

This tool retrieves web hosting information about websites.

Website: <https://myip.ms/>

### Ghostery

A web browser extension that identifies and monitors trackers on any website on the internet.

Website: <https://www.ghostery.com/>

### Security Headers.

This online tool analyses HTTP response headers of a website and rates them depending on the number of headers that the site has. HTTP headers provide high levels of protection and it's important for websites to deploy them.

Website: <https://securityheaders.com/>

# Tech Analysis

## Design and approach

### Dynamic Analysis

Following the static analysis that we carried out using the Exodus Privacy Tool to identify the trackers that the mobile apps use, we took an extra step to investigate the data that these trackers actually transmit. We used an interception environment and an android emulator to carry out the analysis.

### NOTE

According to the findings while we were conducting static analysis using the Exodus Privacy Tool, some mobile applications had Facebook trackers like Facebook Share, Facebook Places, and Facebook Analytics. The tools we used could not identify and analyse the traffic transmitted by these apps because Facebook is currently blocked in Uganda.

### Defining trackers

A tracker is a piece of software meant to collect data about you or your usages. Trackers are created differently, meaning that they do not have same, but have different functions. For example, trackers present Tok-tok different levels of intrusions. Uganda.

## Examples of trackers and their functions are highlighted below

**Crash reporters:** these trackers specialize in reporting application crashes. In other terms, their goal is to notify application developers that an app encountered a problem. As such, information collected at the time the application crashed will allow the developer to correct the bug.

**Analytics:** these trackers are meant to collect data usage and allow the developer to have better knowledge of their audience (for instance, to know what page you visited, or how long you remained on a given area of the page).

**Identification:** these trackers are responsible for determining your digital identity. This identity may refer to an official identity or to abstract identifiers (pseudonym, etc.). The goal will be, for example, to be able to correlate an individual's online and offline activities.

**Ads:** these trackers aim to identify the application user in

order to serve them targeted ads. This is only possible and relevant if the user already Tok-tok has a digital profile established. The goal of the creator of such a tracker is to monetize their application, i.e. to make money by means of advertisement.

**Profiling:** these trackers' goal is to gather as much information as possible on the application user in order to build a virtual profile. To this effect, the tracker will for instance focus on the browsing history, or on the list of installed applications, and so on.

**Location:** these trackers are designed to determine the geographical location of the mobile device. In order to do so, this type of tracker takes advantage of several sensors: GPS chips, surrounding cellular antennae, wi-fi networks present in the area, nearby Bluetooth beacons, or even specific sounds transmitted by loudspeakers.

# Apps have permissions, some of which are indicated as dangerous.

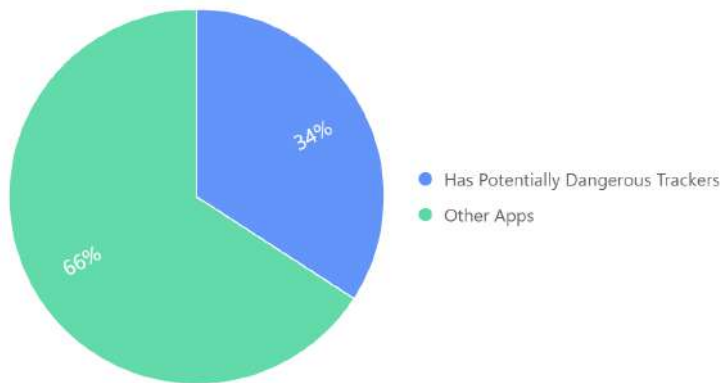
## What is considered potentially dangerous apps?

Google defines danger levels for permissions. Potentially dangerous apps are apps with location trackers / profiling trackers or request user for over 150 permissions. Many dangerous permissions access private user data, a special type of restricted data that includes potentially sensitive information.

Unwanted witness evaluated some of the dangerous apps as detailed below. UW tested 82 apps, among them 28 had profiling or location trackers.

Unwanted witness evaluated some of the dangerous apps as detailed below. UW tested 82 apps, among them 28 had profiling or location trackers.

Percentage of apps with potentially dangerous trackers



### Potentially Dangerous Applications

Potentially dangerous apps are apps with location trackers / profiling trackers or request user for over 150 permissions

Application Name	Number of trackers detected	Number of permissions required	Profiling or Location Trackers detected	Country
Airtel TV	24	22	AppLovin	India
CallApp Contacts	21	53	Verizon Ads	Israel
Clean Master Ultra	17	37	HMS Core & AppLovin	US
King James Bible	15	33	AppLovin	China
WiFi passwords by Instabridge	14	26	AppLovin	Sweden
Junk Removal	13	30	AppLovin	Russia
PoMelo File Explorer - File Manager & Cleaner	13	28	AppLovin	HK
ONE BOOSTER	12	25	AppLovin	Canada
Glovo	12	19	Braze	Spain
Bolt	12	18	Segment & CleverTap	Estonia
Worst Vpn	12	14	AppLovin	Canada
Chipper Cash	11	23	Amplitude	US
Bear VPN	11	17	AppLovin	HK
REAL FOOTBALL	11	14	AppLovin	France
BOTIM - Unblocked Video Call and Voice Call	10	72	HMS Core & Countly	US
Ayoba	10	51	HMS Core	South Africa
Opera Mini	10	29	LeanPlum	Norway
Xender	8	156	HMS Core	China
Alibaba.com	8	36	HMS Core	China
PLAYit	8	25	HMS Core & Kochava	India
Standard/Stanbic Bank	7	31	Audience Studio & HMS Core	South Africa
Thunder VPN	5	11	AppLovin	US
Secure VPN	5	11	AppLovin	US
SafeBoda	5	9	Amplitude & CleverTap	uganda
Showmax	4	13	Braze	Netherlands
Car Driving School 2021	4	8	GameAnalytics	Pakistan
Absa Uganda	1	10	Appdynamics	South Africa
SHAREit Lite	9	180		Singapore

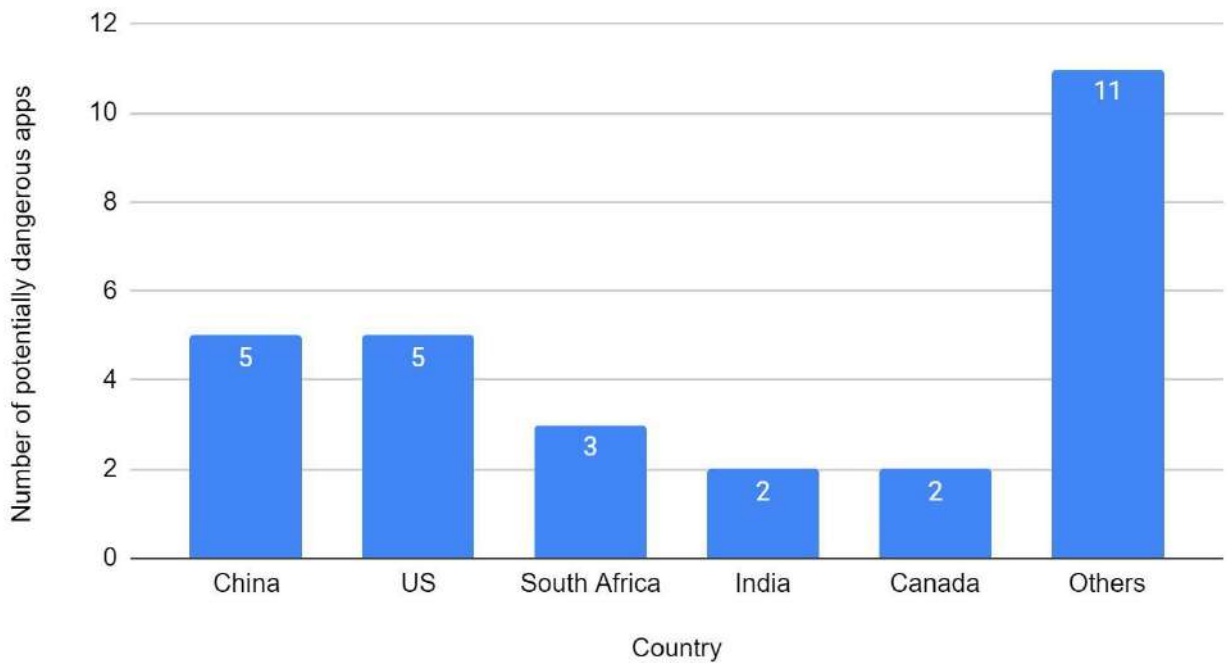
Three of the apps are from South Africa, the others are from Nigeria, Uganda, Spain and Estonia respectively. In Uganda, examples of apps with location trackers include:

- Glovo,
- Safeboda,
- Bolt,
- Standard Bank
- Jumia Food,
- Safeboda,
- Bolt,
- Stanbic Bank,
- Absa Uganda

Those with profiling trackers are listed as;

Notably, Jiji.ug, KiKUU, and Airtel are requiring much more permissions and dangerous permissions compared to similar apps.

### Origins of Apps with potentially dangerous trackers



Countries where the highest potentially dangerous apps are from include:

US, China and South Africa

## Top apps in Uganda

In this report, an analysis of the top apps in Uganda reveals 3 categories of dangerous apps as shown below:

### 1. Top apps requiring over 100 permissions (2 out of 66)

- SHAREit Lite,
- Xender

SHAREit and Xender, among popular apps in Uganda are considered malicious.

- Apart from requiring over 150 permissions from users, SHAREit and Xender are also two file sharing applications that are among top malicious apps identified and blocked by Secure-D , a leading anti-fraud platform. Secure D has detected suspicious activities from these apps.
- These kind of apps can cause fraud transactions or automated clicking activities that further causes data depletion for users

### 2. As Top apps with location tracker (9 out of 66)

- Clean Master Ultra,
- Ayoba,
- Xender,
- Showmax,
- PLAYit,
- Opera Mini,
- BOTIM,
- CallApp Contacts,
- Alibaba.

### 3. Top apps with Profiling Tracker (18 out of 66)

- Clean Master Ultra,
- King James Bible,
- Ayoba,
- uLesson,
- Chipper Cash,
- Opera Mini,
- Airtel TV,
- Jiji.ug,
- NBS TV UGANDA,
- REAL FOOTBALL,
- Junk Removal,
- CallApp Contacts,
- Files,
- Instabridge,
- CamScanner,
- Bear VPN,
- Worst Vpn,
- Bubble Shooter

Application Name	Number of trackers detected	Number of permissions required	Country
TikTok	8	66	China
Phoenix Browser -Video Download, Private & Fast	8	65	China
imo video calls and chat	7	65	US
Facebook	6	59	US
WhatsApp	1	57	US
WhatsApp Business	1	56	US
Telegram	1	55	UK/US
Snapchat	2	44	US
Twitter	4	42	US
Messenger Lite	1	41	US
Instagram	3	37	US
Jiji.ug	12	35	Nigeria
Boomplay	8	33	HK
Uber	4	32	US
Zoom	1	31	US
Spotify	9	29	Sweden
Chat Style	5	29	
My Airtel	3	29	India
Antivirus Master	5	28	China
Jumia Food	10	21	Nigeria
Adobe Scan	7	19	US
Google Meet	1	19	US
VLC for Android	0	18	France
CamScanner	15	17	China
Mystery Lite	5	17	Singapore
uLesson	10	16	Nigeria
StarTimes ONE	3	15	China
MyMTN	2	15	South Africa
Shazam	2	14	US
Jumia	9	13	Nigeria
MTN MoMo	1	12	South Africa
MTN Pulse	1	12	South Africa
Bubble Shooter	20	11	Israel
Candy Crush Saga	7	11	Malta
YOTVs	4	11	Uganda
DroidVPN	2	11	Philippines
Water Color Sort	5	10	Vietnam
NBS TV UGANDA	10	9	Uganda
Matatu	3	8	Uganda
OperaFootball	3	8	Norway
Live Football Tv	9	6	Pakistan
HD Video Projector Simulator	1	6	Unknown

Tracker & Permission info for other popular applications

## Tracker & Permission info for other popular applications

Notably, a few Apps stand out as the Apps with the most trackers. And these include:

- Airtel TV (24),
- CallApp Contacts (21),
- Bubble Shooter(20)
- CallApp Contacts

- Phone cleaning apps e.g. Clean Master Ultra, a file cleaning app from US has 17 trackers including all types of trackers.
- King James Bible, a Bible reading app requires 33 permissions and has 15 trackers, including profiling trackers (why would a reading app requires so many permissions, trackers)

### Conclusions

Other unique apps that people may never suspect to be dangerous include:

- Caller ID app from Israel has 21 trackers including all types of trackers. The app while giving you info about the person calling you, also read your data of course.
- Four out of Five VPN apps have potentially dangerous trackers.

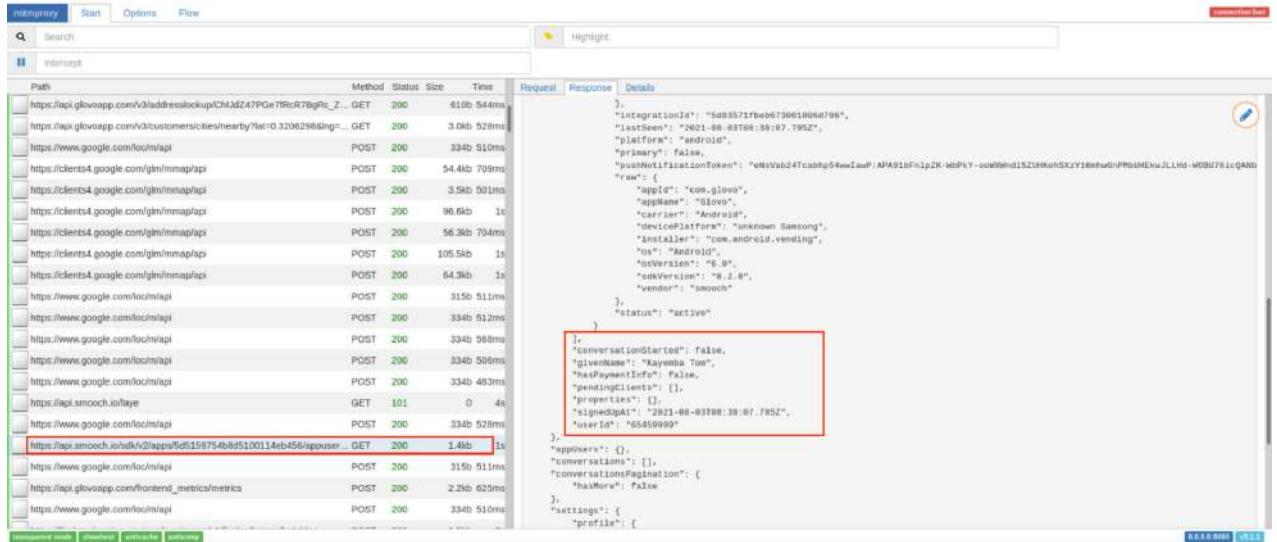
Apps with dangerous trackers include those with unsuspecting functions such as; file sharing, file scanner, phone cleaning & file management, gaming, VPN, instant messaging, online shopping, media player, browser, fintech, callerID, wifi password decoder. Think of the trackers grabbing your info while you try to read Bible, clean your phone, use VPN or sharing a file, etc.

# 1. E-commerce app assessment

# Glovo

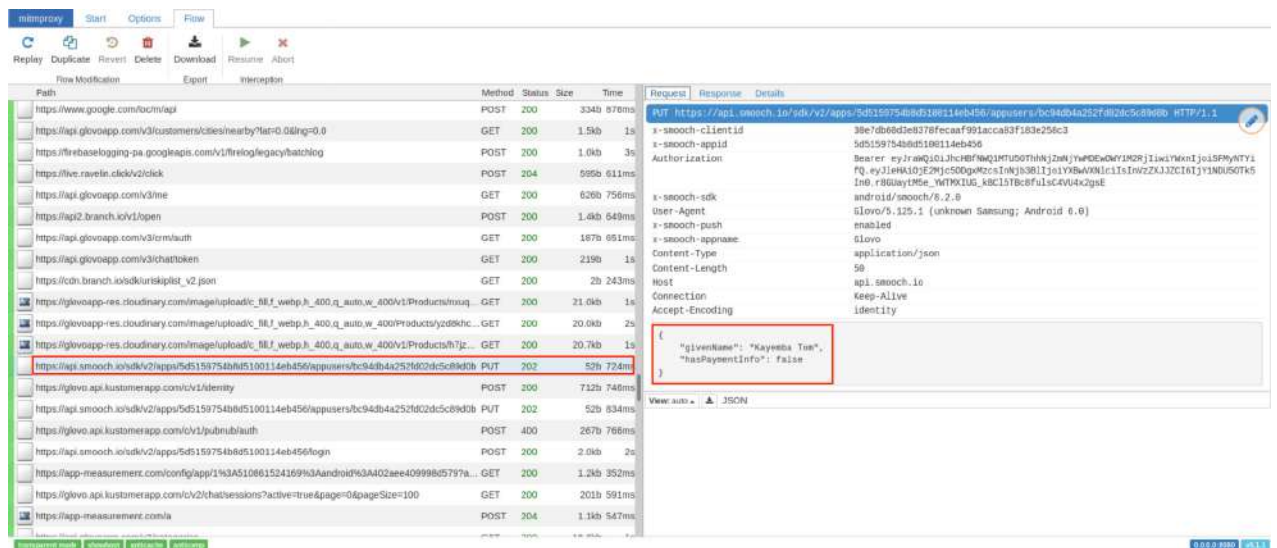
## Findings (3rd August 2021)

The application uses the trackers discovered by Exodus Privacy Tool. On intercepting the information transferred by the Glovo mobile app, we found out that a tracker identified as Smooch captured the user's name, phone specs - android version, phone type, manufacturer, SDK version, and device ID. The tracker also captures the time that the user signed up for the account via the application.



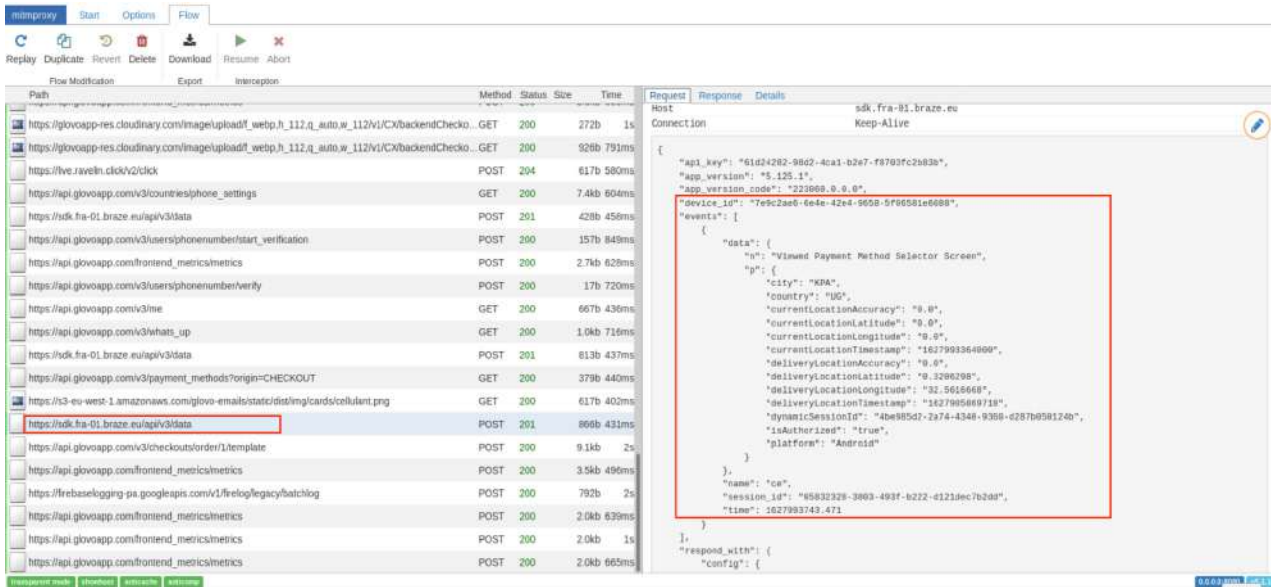
Smooch Technologies Inc. is a tech company based in Montreal, Canada. The Company, through its platform, provides cross channel, live web, in-app, and social messaging services. Website: [www.smooch.io](http://www.smooch.io)

The 'smooch' tracker transmits the user name again during the process of ordering for a product





The ‘smooch’ tracker transmits the user name again during the process of ordering for a product



a. The mobile application had 12 trackers including Facebook trackers like Login, Share and Analytics

<https://www.ssllabs.com/ssltest/analyze.html?d=glovoapp.com>

b) Website.

c. Blacklight markup

SSL server test

Blacklight detected trackers on this page sending data to companies involved in online advertising. Blacklight detected scripts belonging to the companies Facebook, Inc. and Alphabet, Inc.

The SSL servers of Glovo’s website scored A on average

b. Security Headers.

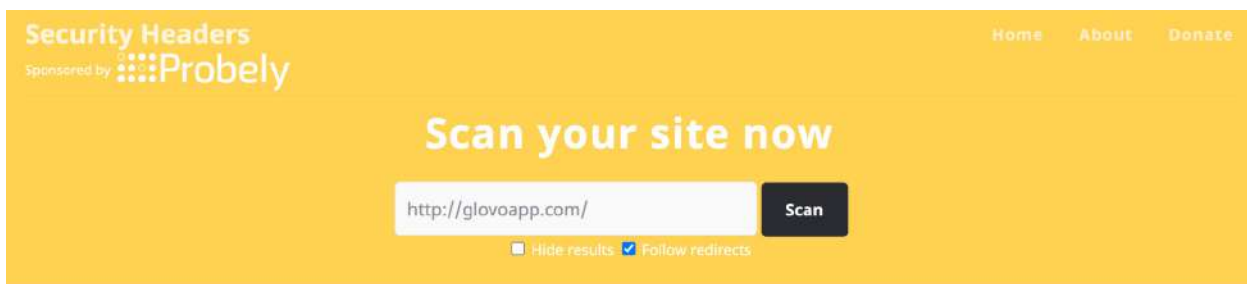
d. MyIP

The website score a C after the assessment. This is because it lacked security headers like strict-transport security, content-security policy and permissions-policy.

The website is hosted on Amazon web servers in Seattle, USA

<https://themarkup.org/blacklight?url=glovoapp.com>

Report: <https://reports.exodus-privacy.eu.org/en/reports/179891/>



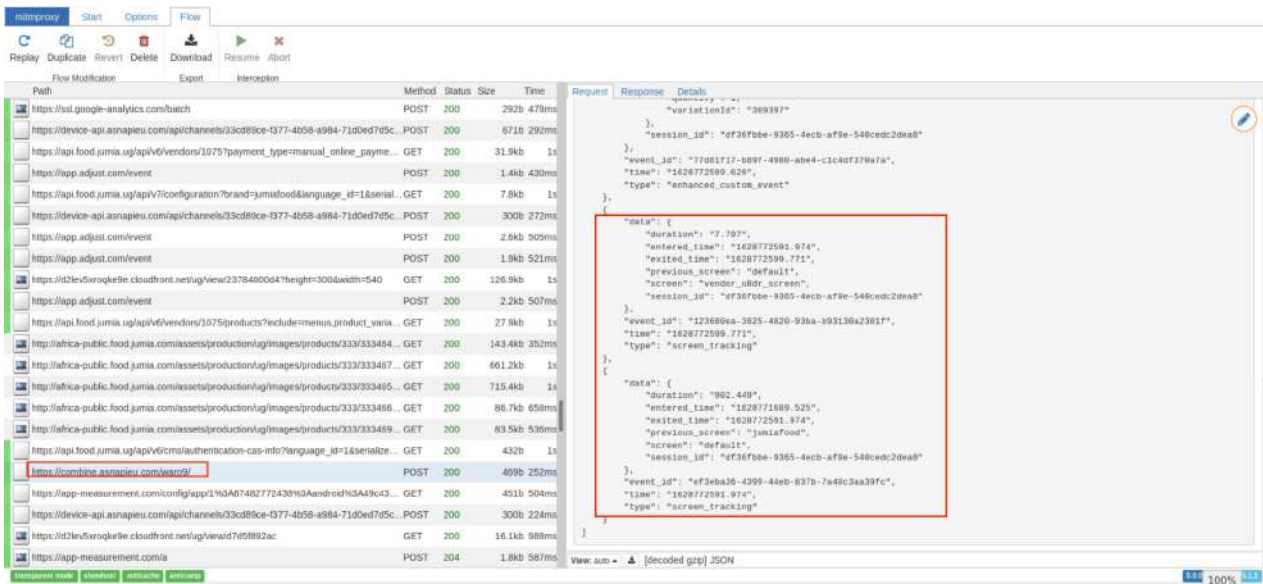
# JUMIA

Findings (4th August 2021)

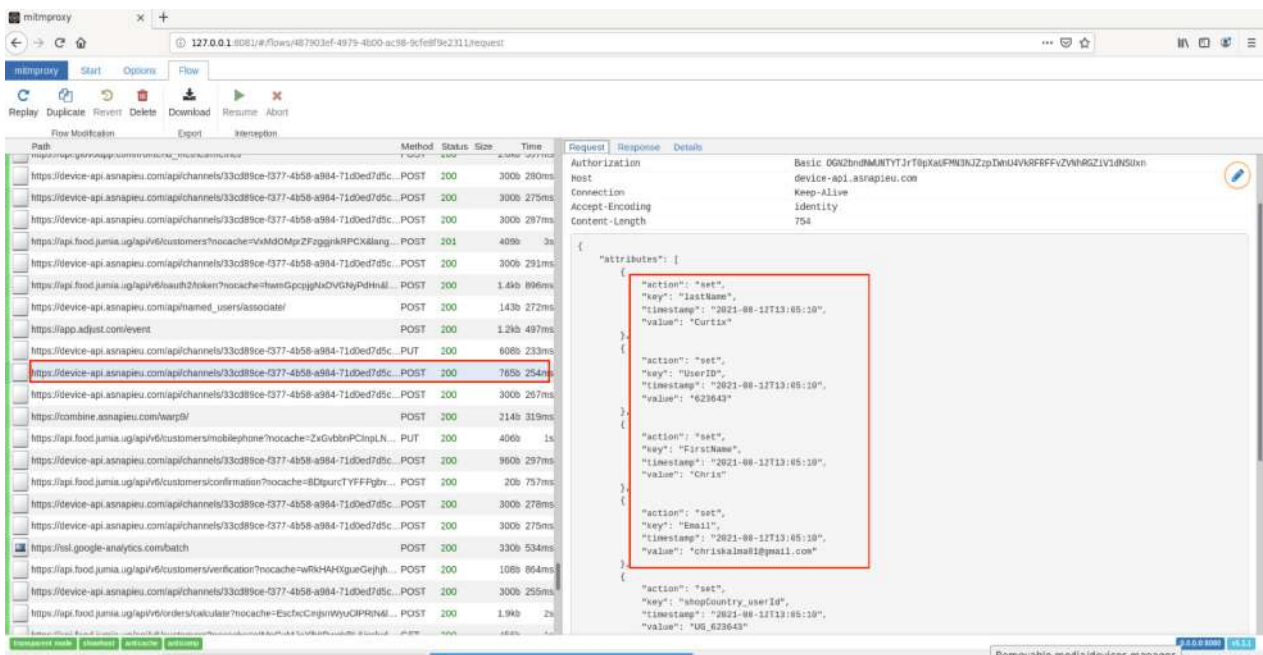
We identified a tracker called 'asnapieu' that captures the user's info like first and last names, gender, and userID

Further investigations revealed that the application uses a tracker known as 'asnapieu' to transmit users' location coordinates. We did a background search and found out that the company is located in San Francisco, USA.

The tracker also tracks the users' activity while interacting with the application also known as screen tracking as illustrated below.

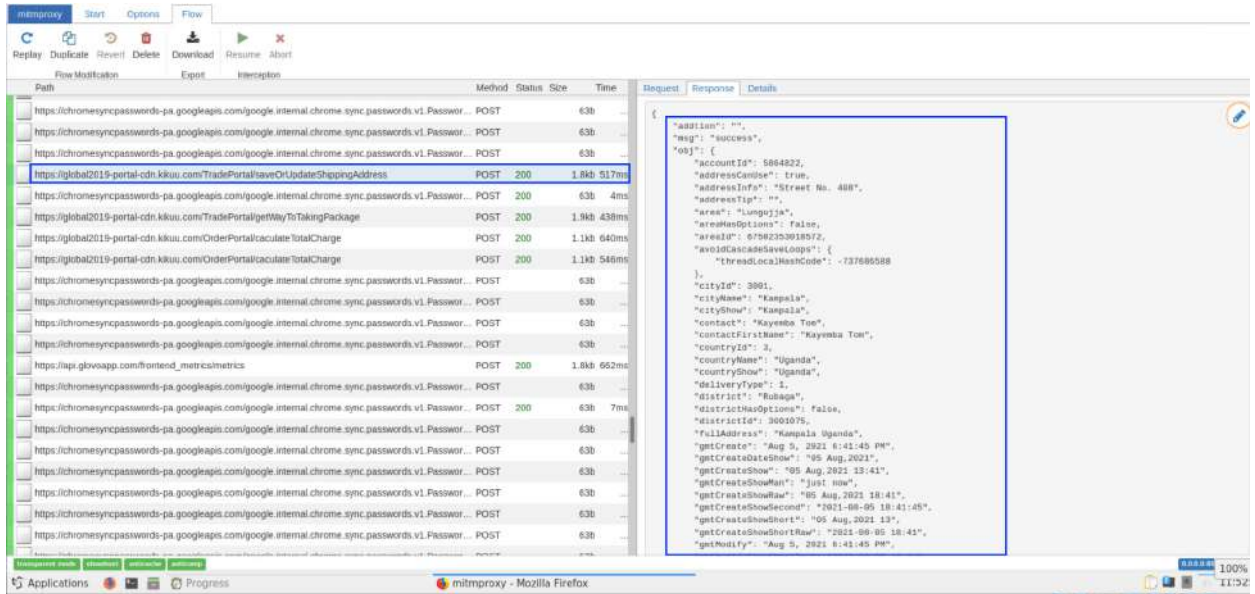


Additionally, the tracker also transfers the users' names, email, country of origin, and advertising ID during the registration stage (when the user is registering for a new account) as illustrated in the screenshot below.



# KiKUU (5th August 2021)

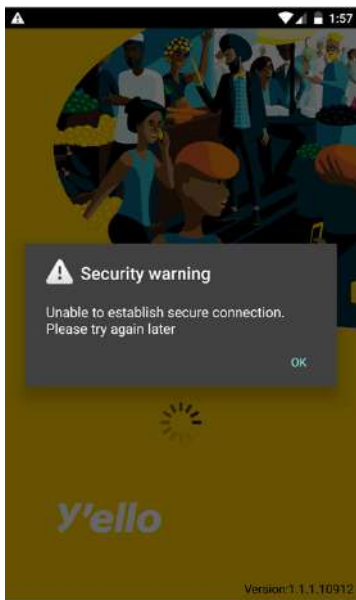
Trackers such as Push and Umeng were identified during the deep analysis of Kikuu mobile app. The few identified trackers were not transferring sensitive users' personal data. Data processing of customers' data is mainly handled on the company's servers. Data collection by KiKUU illustrated in the screenshot below



# MTN MoMo App

(5th August 2021)

The app displayed a pop-up warning after we opened it up for testing. This means that MTN implemented security mechanisms to detect man in the middle attacks thereby hindering us from analyzing what kind of data that the trackers transmit from to the data servers.

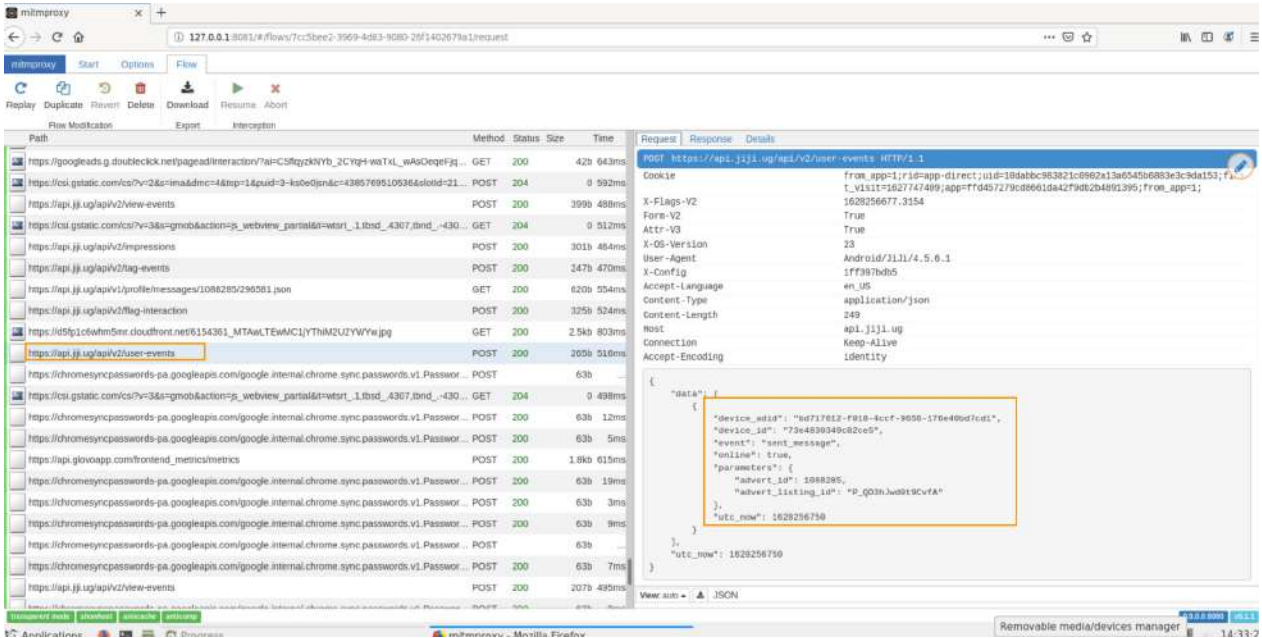


## MyMTN

None of the trackers was transferring users' personal data. All sensitive data was transferred to the domain of MTN

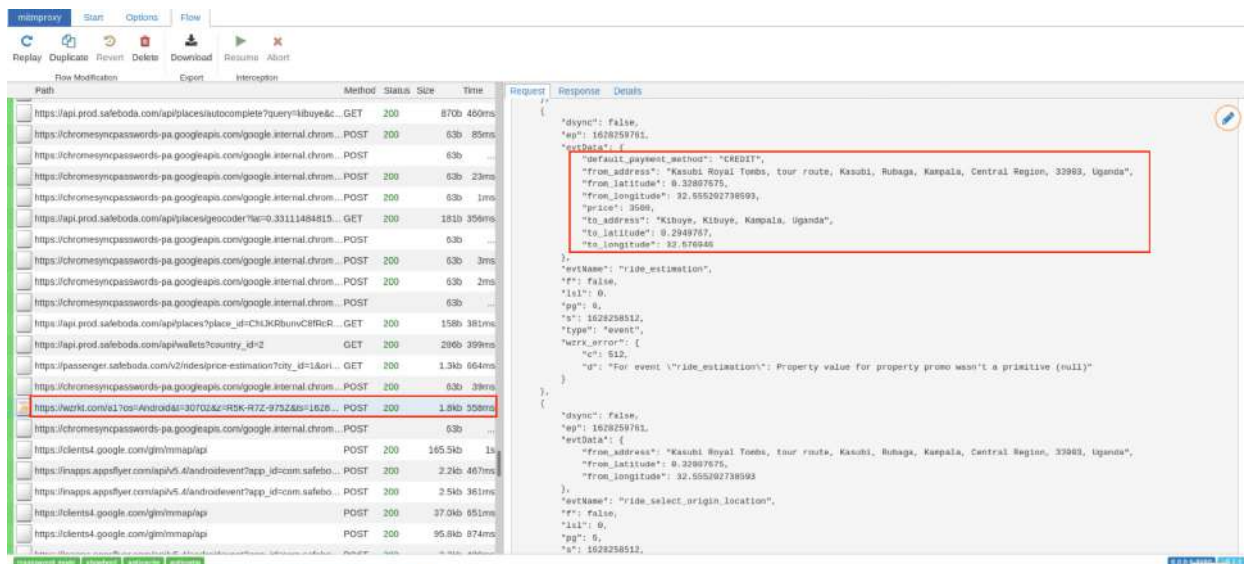
# Jiji.ug Uganda

Few trackers were identified while carrying out the deep analysis of the application such as Appsflyer, and Cloudfront. The transmission of personal data like user's address, contact details are handled on the servers of the company.



# Safeboda

The tracker still transmits users' sensitive location data to wrzkt.com servers as illustrated in the screenshot below.



# Bolt

The company employs 12 trackers in its mobile application. These include but not limited to; CleverTap (used by Safeboda too), AppsFlyer, Facebook Analytics, Places, Flipper, Share and Login as shown in the screenshot here shown.

exodus Home Reports Trackers Better understand The organization en

## Bolt Bolt

**12 trackers** **18 permissions**

Version CA.19.5 - [see other versions](#)  
Source: Google Play  
Report created on Aug. 9, 2021, 11:54 a.m.

[See on Google Play >](#)

### 12 trackers

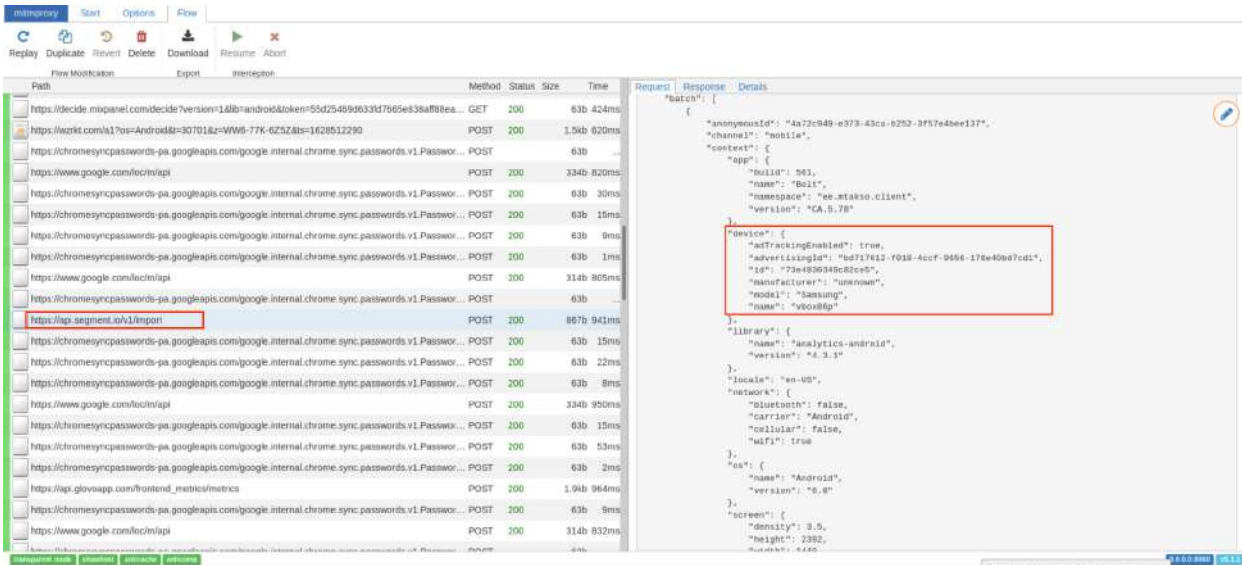
We have found **code signature** of the following trackers in the application:

- AppsFlyer >  
analytics
- CleverTap >  
analytics profiling location
- Facebook Analytics >  
analytics
- Facebook Flipper >  
analytics
- Facebook Login >  
identification
- Facebook Notifications >
- Facebook Share >
- Google CrashLytics >  
crash reporting
- Google Firebase Analytics >  
analytics
- MixPanel >  
analytics advertisement
- Segment >  
analytics profiling
- Tune >  
analytics

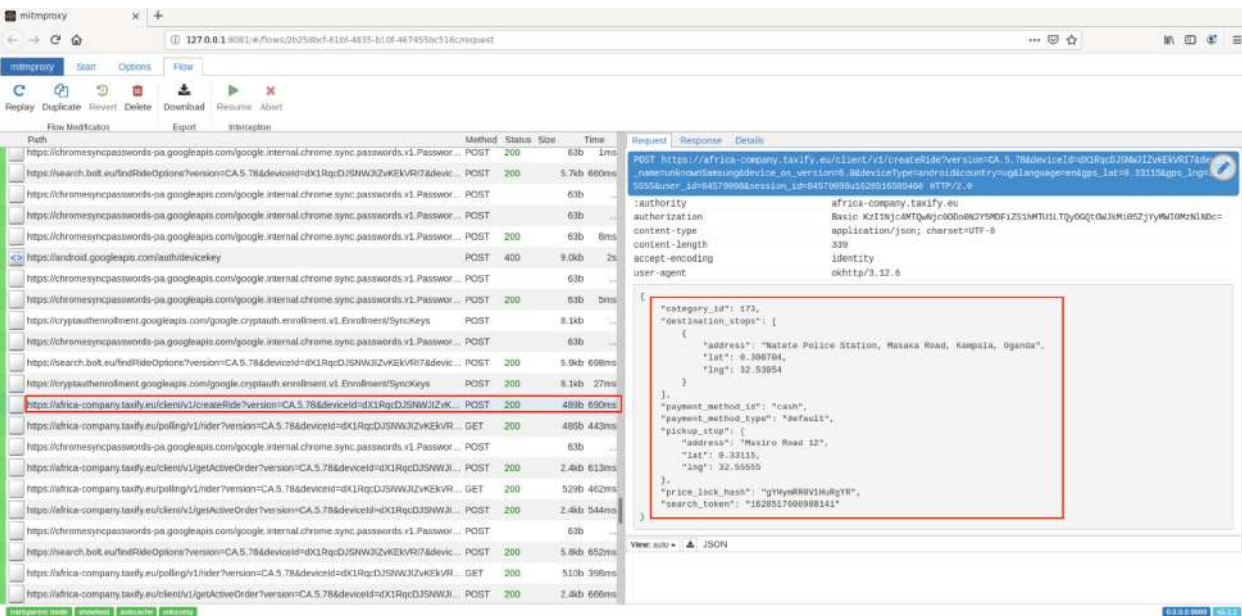
A tracker is a piece of software meant to collect data about you or your usages. [Learn](#)



The company uses the segment tracker to profile users of the application. In the screenshot below, the tracker collects the user's advertising ID and other information about the device.



Processing of users' location data is handled on the company's servers as illustrated in the screenshot below;



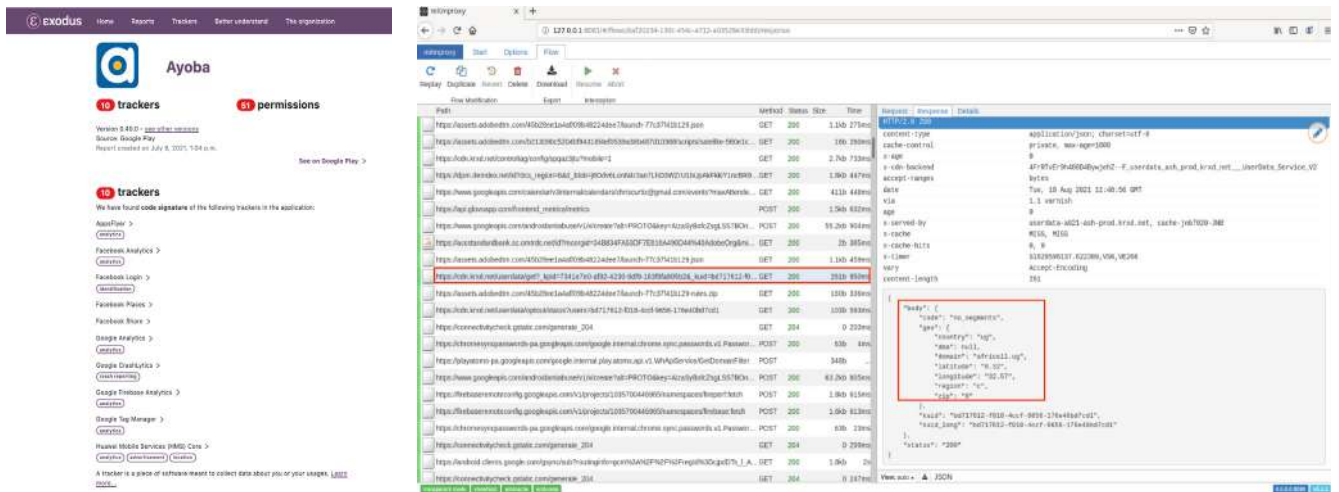
# Ayoba App

Android version of the Ayoba Application using Exodus, the application has ten trackers including Facebook trackers like Facebook Share, Facebook Analytics, Facebook Login and Facebook Places. More so, the application uses Huawei's Mobile Services tracker to collect the location of the users.

<https://reports.exodus-privacy.eu.org/en/reports/com.ayoba.ayoba/latest/>

We identified a tracker known as krxd.net transferring the user's country of origin, broad location coordinates and the name of ISP

NB: Couldn't do more tests using the android emulator. Stuck at the phone number verification stage.



# Masikini

**a. Exodus Privacy:** The application had the following Facebook Trackers; Facebook Login, Facebook share, Facebook Analytics.

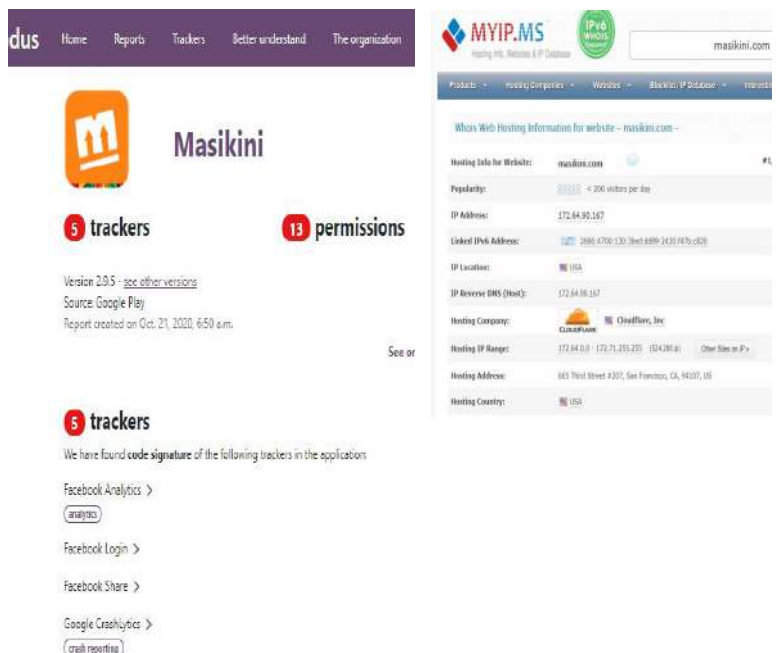
**b. SSL Server test:** The SSL servers of Masikini website scored B on average after the test

**c. Security Headers:** The website scored a D after an analysis by security headers. The SSL certificate missed security headers like Strict Transport Security, Content security policy, referrer policy and permissions policy.

**d. Ghostery:** The website had four trackers including Facebook connect and Hotjar.

**e. MyIP:** The company stores its users' data on servers in San Francisco, USA.

<https://www.ssllabs.com/ssltest/analyze.html?d=masikini.com>

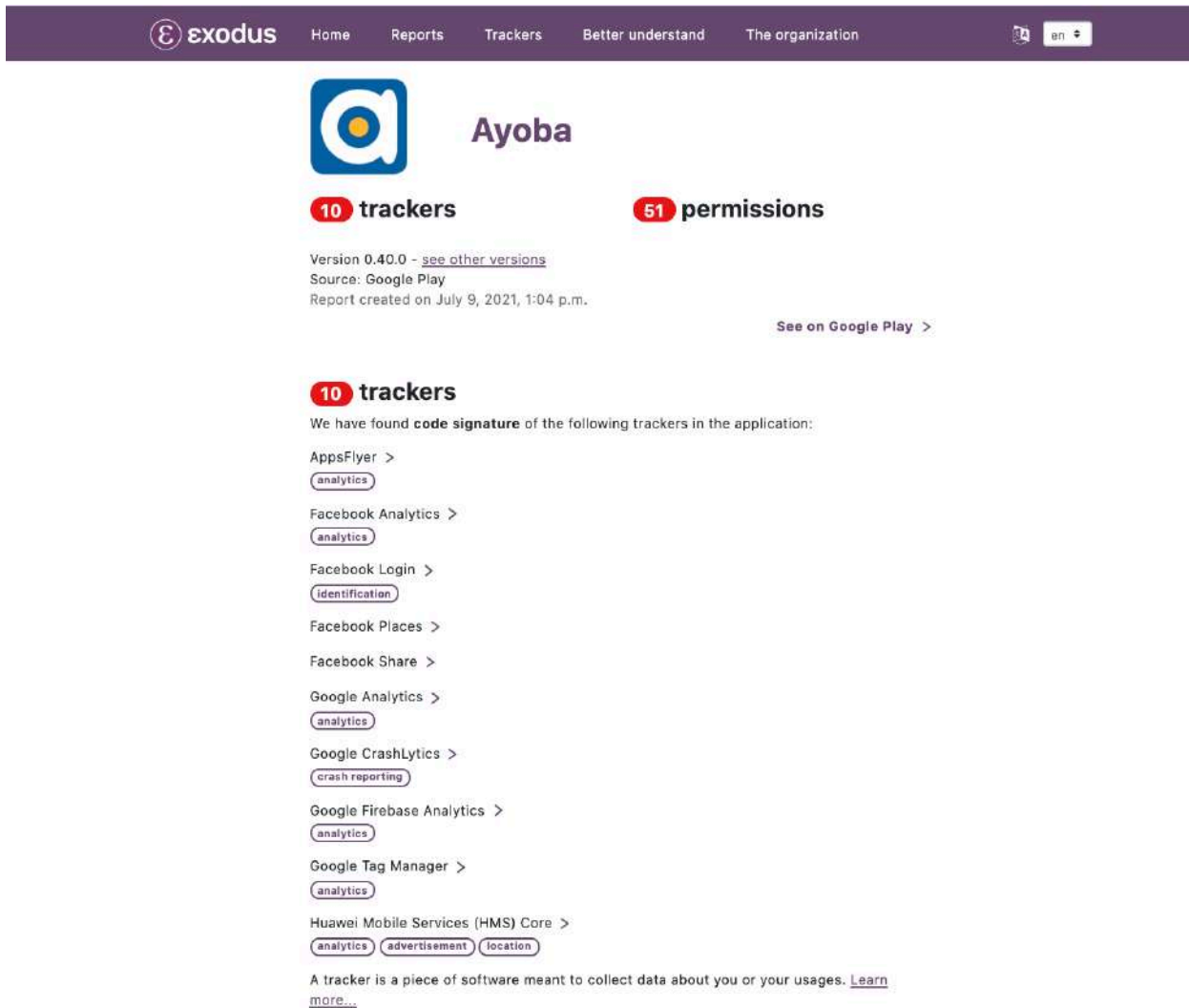




# Ayoba App

According to the findings from the analysis that we carried out on the Android version of the Ayoba Application using Exodus, the application has ten trackers including Facebook trackers like Facebook Share, Facebook Analytics, Facebook Login and Facebook Places. More so, the application uses Huawei's Mobile Services tracker to collect the location of the users.

<https://reports.exodus-privacy.eu.org/en/reports/com.ayoba.ayoba/latest/>



**exodus** Home Reports Trackers Better understand The organization en

## Ayoba

**10 trackers** **51 permissions**

Version 0.40.0 - [see other versions](#)  
 Source: Google Play  
 Report created on July 9, 2021, 1:04 p.m.

[See on Google Play >](#)

### 10 trackers

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

- AppsFlyer > [analytics](#)
- Facebook Analytics > [analytics](#)
- Facebook Login > [identification](#)
- Facebook Places >
- Facebook Share >
- Google Analytics > [analytics](#)
- Google CrashLytics > [crash reporting](#)
- Google Firebase Analytics > [analytics](#)
- Google Tag Manager > [analytics](#)
- Huawei Mobile Services (HMS) Core > [analytics](#) [advertisement](#) [location](#)

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

# FlexiPay

The application didn't have any tracker by the time we carried out the analysis using the Exodus Privacy tool.

<https://reports.exodus-privacy.eu.org/en/reports/187922/>



## FlexiPay

0 trackers

19 permissions

Version 1.1.8 - [see other versions](#)  
 Source: Google Play  
 Report created on July 9, 2021, 1:07 p.m.

[See on Google Play >](#)

### 0 trackers

We have not found **code signature** of any tracker we know in the application.  
 The application could contain tracker(s) we do not know yet.

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

### 19 permissions

We have found the following permissions in the application:

- ! ACCESS\_COARSE\_LOCATION**  
*access approximate location (network-based)*
- ! ACCESS\_FINE\_LOCATION**  
*access precise location (GPS and network-based)*
- ACCESS\_NETWORK\_STATE**  
*view network connections*

App/Company	Tracker status
Absa Uganda	detected the emulator when we clicked on the application
Masikini	Couldn't pass the verification stage (delays in the delivery of the verification codes)
Kikuubo Online	Nothing suspicious, sensitive data is handled by the company's servers
Cente Mobile	Error = Emulator Detected
Standard/Stanbic Bank	Nothing suspicious was identified. All of the sensitive user's data is handled by the bank's servers.

**b. Website**

**SSL Server Test**

Overall, the Jumia website SSL servers scored B after the tests.

**b. Security Headers.**

The website scored a D after it was scanned using the security headers tool. This means that website is susceptible to injection attacks.

The following were the missing headers;

**HTTP Strict Transport Security:** This an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.

**Content Security Policy.** This is an effective measure to protect your site from XSS attacks.

**X-Content-Type-Options.** This stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type.

**Referrer Policy.** This is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

**Permissions Policy:** This is a new header that allows a site to control which features and APIs can be used in the browser.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.Jumia.ug>

**c. Ghostery.**

i. The extension identified three advertising trackers, one social media tracker (Facebook connect) and two site analytics trackers on the official website.

**d. MyIp.ms**

The website’s servers are located in San Francisco, USA. (Data protection laws in USA are weaker compared to those of Europe (GDPA))

The screenshot shows the MyIP.ms website interface. At the top, there is a search bar containing 'www.jumia.ug'. Below the search bar are navigation tabs: 'Products', 'Hosting Companies', 'Websites', 'Blacklist / IP Database', and 'Interesting'. The main content area is titled 'Whois Web Hosting Information for website - www.jumia.ug'. It displays the following information:

- Hosting Info for Website:** www.jumia.ug #2
- Popularity:** 20,000 visitors per day
- IP Address:** 104.16.69.46
- IP Location:** USA
- IP Reverse DNS (Host):** 104.16.69.46
- Hosting Company:** Cloudflare, Inc
- Hosting IP Range:** 104.16.0.0 - 104.31.255.255 (1,048,576 ip) [Other Sites on IP »]
- Hosting Address:** 665 Third Street #207, San Francisco, CA, 94107, US
- Hosting Country:** USA
- Hosting Phone:** +1-650-319-8930

## 2. Financial services app assessment

# Stanbic Bank, Uganda.

## Mobile Application

According to the report by Exodus Privacy, the android application of Stanbic bank Uganda has five trackers namely; Adobe Experience Cloud, Google Crashlytics, Google AdMob, Google Firebase Analytics, and Krux (audience studio). Thirty one app permissions were also recorded from the android app. NOTE: Krux is a piece of software owned by Salesforce (company based in California, USA) that compiles information from the users of the app to create detailed user profiles.

<https://reports.exodus-privacy.eu.org/en/reports/154919/>

**5 trackers**      **31 permissions**

Version 3.23.2 - see other versions  
Source: Google Play  
Report created on Nov. 26, 2020, 10:16 a.m.

**5 trackers**

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

- Adobe Experience Cloud >
- Audience Studio (Krux) >
  - analytics
  - profiling
- Google AdMob >
  - advertisement
- Google Crashlytics >
  - crashreporting
- Google Firebase Analytics >
  - analytics

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

## Website.

The website (www.stanbicbank.co.ug/) employs the latest transport layer security version (1.3) and 128 keys AES encryption standard. We went ahead to test the security of both the SSL server, and the certificate.

## SSL Labs Test by Qualys.

The SSL servers of Stanbic’s website scored A+

<https://www.ssllabs.com/ssltest/analyze.html?d=www.stanbicbank.co.ug>

Server	Test time	Grade
1 <a href="https://104.16.87.99">104.16.87.99</a> Ready	Thu, 26 Nov 2020 10:08:09 UTC Duration: 02: 779 sec	A+
2 <a href="https://104.16.86.99">104.16.86.99</a> Ready	Thu, 26 Nov 2020 10:09:42 UTC Duration: 03: 725 sec	A+
3 <a href="https://2606:4700:0:0:0:6810:5663">2606:4700:0:0:0:6810:5663</a> Ready	Thu, 26 Nov 2020 10:11:15 UTC Duration: 08: 504 sec	A+
4 <a href="https://2606:4700:0:0:0:6810:5763">2606:4700:0:0:0:6810:5763</a> Ready	Thu, 26 Nov 2020 10:12:44 UTC Duration: 00: 005 sec	A+

## Security Headers.

Although the website lacked security headers like X-Content-Type-Options and Permissions-Policy, its grade was capped at A.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.stanbicbank.co.ug%2F&followRedirects=on>

**Security Report Summary**

Site: <https://www.stanbicbank.co.ug/>

IP Address: 2606:4700:0:6810:5663

Report Time: 26 Nov 2020 10:08:19 UTC

Headers:
 

- ✔ Strict-Transport-Security
- ✔ Content-Security-Policy
- ✔ Referrer-Policy
- ✔ X-Frame-Options
- ✘ X-Content-Type-Options
- ✘ Permissions-Policy

Warning: Grade capped at A, please see warnings below.

## Blacklight Markup

Five third-party cookies were found on this website. Blacklight detected cookies set for Verizon Media, Adobe Inc. and Alphabet, Inc. More so, the tool detected scripts of trackers belonging to the companies Adobe Inc. and Alphabet, Inc.

## MyIp

The website is hosted on a server in San Francisco, USA

<https://themarkup.org/blacklight?url=www.stanbicbank.co.ug>, <https://myip.ms/info/whois/104.16.86.99/k/3085277320/website/www.stanbicbank.co.ug>

# Standard Chartered Bank, Uganda.

## Mobile Application

According to a report by Exodus Privacy, the android app contain six trackers, namely; Google Analytics, Google Crashlytics, Google Firebase, Google tag manger and MixPanel.

NOTE: MixPanel is a USA based web-analytics company that brands itself as a company that explores user behaviors from all angles.

<https://mixpanel.com/behavioral-analytics/>

**Website:** The website is encrypted with AES 256 keys, and runs the latest TLS version (1.3). To analyze further the security of the website, we used the following tools;

### SSL Server Lab Test

The SSL server of the website scored A+ when it was put to test by Qualys SSL lab tool.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.sc.com>

**6 trackers**      **42 permissions**

Version 5.10.0 - [see other versions](#)  
 Source: Google Play  
 Report created on Nov. 26, 2020, 2:09 p.m.

[See on Google Play >](#)

**6 trackers**

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

- Adobe Experience Cloud >
- Google Analytics Cloud >
- Google Analytics >
- Google Crashlytics >
- Google Firebase Analytics >
- Google Tag Manager >
- MixPanel >

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

**Qualys. SSL Labs**      Home    Projects    Qualys Free Trial    Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.sc.com](#)

**SSL Report: www.sc.com**

Assessed on: Thu, 26 Nov 2020 14:16:30 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

Server	Test time	Grade
1 <a href="#">104.68.101.222</a> s104-68-101-222.deploy.static.akamaitechnologies.com Ready	Thu, 26 Nov 2020 14:13:35 UTC Duration: 48.114 sec	A+
2 <a href="#">2600:1408:7400:4b6:0:0:0:6dc</a> g2600-1408-7400-04b6-0000-0000-0000-0000.deploy.static.akamaitechnologies.com Ready	Thu, 26 Nov 2020 14:14:23 UTC Duration: 68.662 sec	A+
3 <a href="#">2600:1408:7400:4aa:0:0:0:6dc</a> g2600-1408-7400-04aa-0000-0000-0000-0000.deploy.static.akamaitechnologies.com Ready	Thu, 26 Nov 2020 14:15:32 UTC Duration: 67.143 sec	A+

SSL Report v2.1.8

**2. Security Headers:** The website had two essential missing security headers. The grade was capped to A.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.c.com%2Fug%2F&followRedirects=on>

**Security Headers**  
Sponsored by **Probely**

Home    About    Donate

**Scan your site now**

Hide results     Follow redirects

**Security Report Summary**

**A**

Site: <https://www.sc.com/ug/>

IP Address: 2600:1408:7400:397:3cc

Report Time: 26 Nov 2020 14:13:41 UTC

Headers:

- Content-Security-Policy
- Strict-Transport-Security
- X-Frame-Options
- X-Content-Type-Options
- Referrer-Policy
- Permissions-Policy

### Blacklight Markup

Blacklight detected six trackers and 10 cookies on the website sending data to companies involved in online advertising. Blacklight detected scripts belonging to Alphabet, Inc., Facebook, Inc., and LinkedIn Corporation.

### MyIPs

The hosting server is located in California, USA.

<https://themarkup.org/blacklight?url=www.sc.com>

# Centenary Bank, Uganda

**Mobile Application:** We carried out a static analysis on the CenteMobile app using Exodus Privacy and we identified 5 trackers in the android mobile application. These included; Facebook Places, Facebook Login and Facebook Share. NOTE: There have been concerns over these trackers for sharing information back to the Facebook servers without users' consent.

<https://reports.exodus-privacy.eu.org/en/reports/154942/>

**5 trackers**      **17 permissions**

Version 76.6 - [see other versions](#)  
 Source: Google Play  
 Report created on Nov. 26, 2020, 3:34 p.m.

[See on Google Play >](#)

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

**Website:** Verified by DigiCert Inc, the website is encrypted with 256 keys AES and uses version 1.2 of transport layer security. To further test the security of the website, we used the following tools;

**SSL Lab Server Test:** The SSL server of the website scored a B because it supports weak Diffie-Hellman (DH) key exchange parameters and also supports older versions of TLS that is; TLS 1.0 and TLS 1.1.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.centenarybank.co.ug>

**Qualys. SSL Labs**      Home    Projects    Qualys Free Trial    Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.centenarybank.co.ug](#)

**SSL Report: www.centenarybank.co.ug (13.95.192.56)**

Assessed on: Thu, 26 Nov 2020 15:38:00 UTC | [Hide](#) | [Clear cache](#)      [Scan Another »](#)

**Summary**

Overall Rating

**B**

Certificate	100%
Protocol Support	80%
Key Exchange	80%
Cipher Strength	90%

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

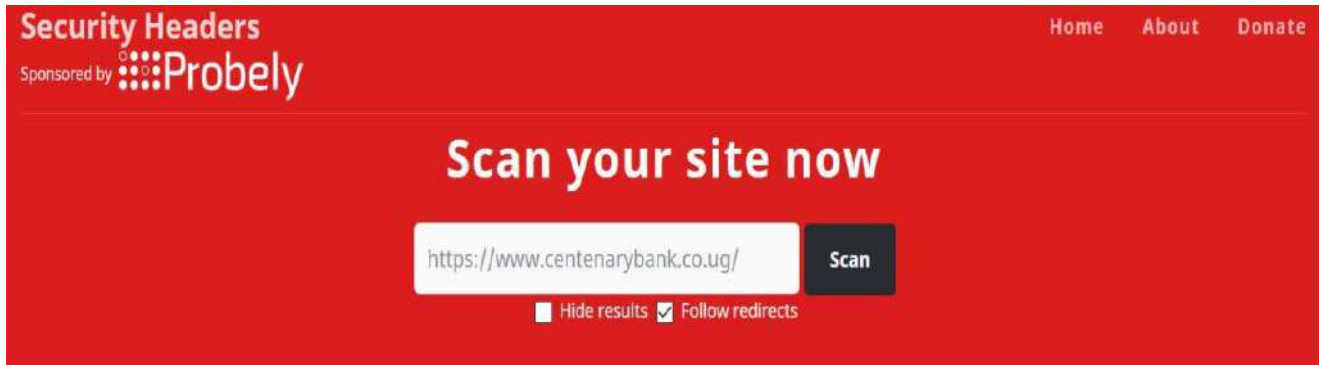
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

# Centenary Bank, Uganda

**Mobile Application:** We carried out a static analysis on the CenteMobile app using Exodus Privacy and we identified 5 trackers in the android mobile application. These included; Facebook Places, Facebook Login and Facebook Share. NOTE: There have been concerns over these trackers for sharing information back to the Facebook servers without users' consent.

<https://reports.exodus-privacy.eu.org/en/reports/154942/>



**3. Blacklight Markup:** Blacklight detected scripts belonging to the companies Alphabet, Inc., Microsoft Corporation and Facebook, Inc. and one cookie set for Zendesk, Inc.

**4. Mylps:** The server that hosts [www.centenarybank.co.ug](http://www.centenarybank.co.ug) domain are located in Redmond, USA.

<https://themarkup.org/blacklight?url=www.centenarybank.co.ug>



# ABSA Bank, Uganda (Formerly Barclays)

**Mobile Application:** We identified trackers owned by Alphabet Inc. (Google), Microsoft and New Relic (used for analytics)

**5 trackers**      **13 permissions**

Version 6.1.7 - [see other versions](#)  
 Source: Google Play  
 Report created on Oct. 5, 2020, 2:09 p.m. and updated on Oct. 7, 2020, 2:09 p.m.  
[See on Google Play >](#)

**5 trackers**

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

Google Crashlytics >

**Website:**

**SSL Lab Server Test:** The website employs version 1.2 of the transport layer security (TLS) and verified by DigiCert Inc. The three SSL servers of the website scored A on average.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.absa.co.ug>

**Qualys. SSL Labs**      Home    Projects    Qualys Free Trial    Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.absa.co.ug](#)

**SSL Report: www.absa.co.ug**  
 Assessed on: Fri, 27 Nov 2020 07:33:06 UTC | [Hide](#) | [Clear cache](#)      [Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">52.49.105.66</a> ec2-52-49-105-66.eu-west-1.compute.amazonaws.com Ready	Fri, 27 Nov 2020 07:27:08 UTC Duration: 119.521 sec	A
2	<a href="#">46.51.204.150</a> ec2-46-51-204-150.eu-west-1.compute.amazonaws.com Ready	Fri, 27 Nov 2020 07:29:07 UTC Duration: 119.407 sec	A
3	<a href="#">52.213.30.91</a> ec2-52-213-30-91.eu-west-1.compute.amazonaws.com Ready	Fri, 27 Nov 2020 07:31:07 UTC Duration: 119.218 sec	A

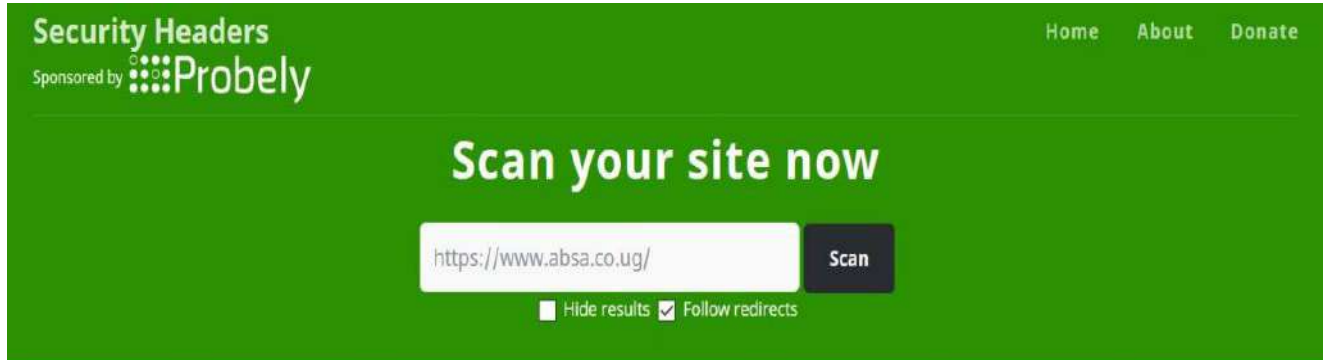
SSL Report v2.1.8

**Website:**


**2. Security Headers**

The website's grade was capped A - because it lacked the Permissions-policy security header.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.absa.co.ug%2F&followRedirects=on>



**Security Report Summary**

	Site:	<a href="https://www.absa.co.ug/personal/">https://www.absa.co.ug/personal/</a>
	IP Address:	46.51.204.150
	Report Time:	27 Nov 2020 07:27:04 UTC
	Headers:	<span>✔ Strict-Transport-Security</span> <span>✔ X-Content-Type-Options</span> <span>✔ Referrer-Policy</span> <span>✔ Content-Security-Policy</span> <span>✔ X-Frame-Options</span> <span>✘ Permissions-Policy</span>
	Warning:	Grade capped at A, please see warnings below.

**Blacklight Markup**

Blacklight detected nine trackers and 11 third-party cookies on the website sending data to companies involved in online advertising. Blacklight detected scripts belonging to Facebook, Inc., Alphabet, Inc., and LinkedIn Corporation.

The website uses Facebook Pixel. This is a snippet of code that sends data back to Facebook about people who visit this site and allows the site operator to later target them with ads on Facebook.

**MyIP**

The website is hosted on Amazon servers in Ireland <https://themarkup.org/blacklight?url=absa.co.ug>

# DFCU Bank, Uganda.

Mobile Application.

Using Exodus Privacy to carry-out a static analysis, we found only one tracker in DFCU’s Quick App. The tracker belonged to Alphabet Inc.

<https://reports.exodus-privacy.eu.org/en/reports/154982/>

**dfcu QuickApp**

**1 tracker**      **21 permissions**

Version 2.0.0 - [see other versions](#)  
 Source: Google Play  
 Report created on Nov. 27, 2020, 7:55 a.m.

[See on Google Play >](#)

**1 tracker**

We have found **code signature** of the following tracker in the application:

Google CrashLytics >  
 crash reporting

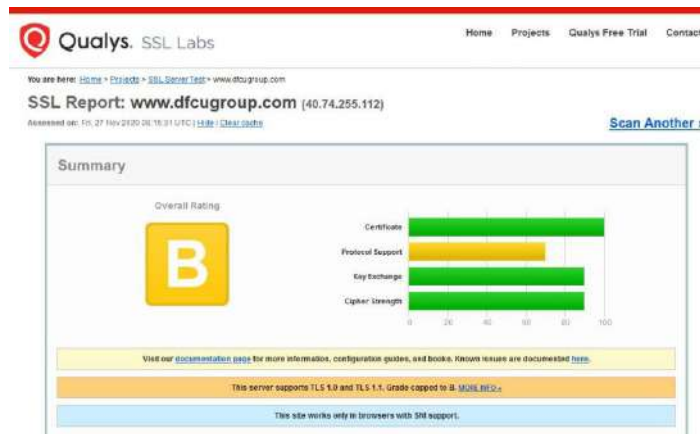
## Website.

The website’s SSL certificate is verified by GoDaddy.com Inc and runs version 1.2 of the transport layer security (TLS).

## SSL Lab Server Test

Basing on the report by Qualys SSL server testing tool, the website scored a B due to the fact that it supports versions 1.0 and 1.1 of the transport layer security (TLS) protocol.

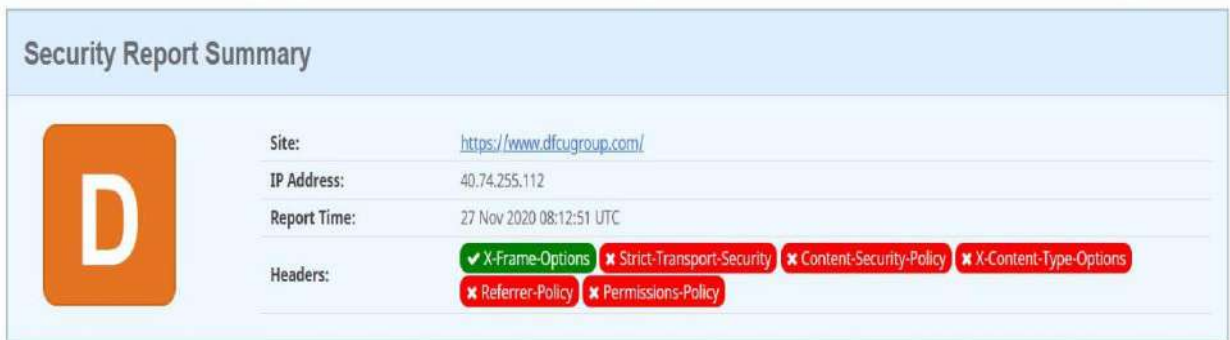
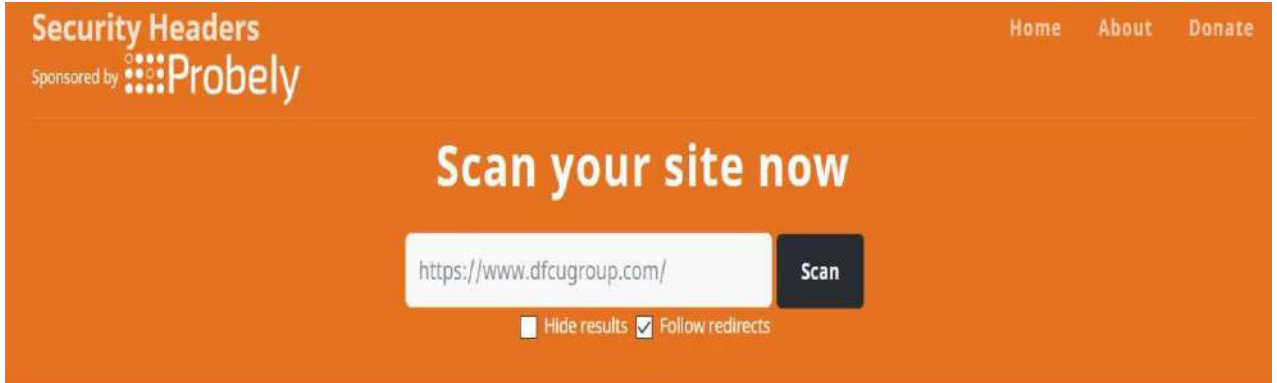
<https://www.ssllabs.com/ssltest/analyze.html?d=www.dfcugroup.com>



## 2. Security Headers

According to a report by securityheaders.io, DFCU's website has missing security headers. This puts the website at risk of cyber-attacks like Click-jacking and injection attacks.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.dfcugroup.com%2F&followRedirects=on>



## 3. Blacklight Markup

Three trackers and one cookie owned by Alphabet Inc. (Google) were identified on the website, according to a report by Blacklight. Furthermore, the website uses key logging on some fields.

**NOTE:** Key logging is when a website captures the text that you type into a webpage before you hit the submit button.

The website captured key-strokes of the users; information entered in the name, family-name, given-name fields on the website.

## 4. MyIp

The website is hosted on a Microsoft server in Texas, USA.

<https://themarkup.org/blacklight?url=www.dfcugroup.com>

# 3. Government Agencies app assessment

# Ministry of Health, Uganda.

In this analysis, we focused on only the website (<https://www.health.go.ug/>) since the institution doesn't have an official mobile application.

## SSL Lab Server Test

Overall, the website SSL server scored a B after it was tested by Qualys SSL Lab server testing tool.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.health.go.ug>

The screenshot shows the SSL Labs report for www.health.go.ug, assessed on Tue, 24 Nov 2020 13:11:23 UTC. The report includes a 'Scan Another >>' link and a table with the following data:

	Server	Test time	Grade
1	<a href="https://2606:4700:20:0:0:ac43:4768">2606:4700:20:0:0:ac43:4768</a> Ready	Tue, 24 Nov 2020 13:00:46 UTC Duration: 105.545 sec	B
2	<a href="https://2606:4700:20:0:0:681a:c31">2606:4700:20:0:0:681a:c31</a> Ready	Tue, 24 Nov 2020 13:02:30 UTC Duration: 104.445 sec	B
3	<a href="https://2606:4700:20:0:0:681a:d31">2606:4700:20:0:0:681a:d31</a> Ready	Tue, 24 Nov 2020 13:04:16 UTC Duration: 104.201 sec	B
4	<a href="https://104.26.12.49">104.26.12.49</a> Ready	Tue, 24 Nov 2020 13:05:59 UTC Duration: 108.437 sec	B
5	<a href="https://172.67.71.104">172.67.71.104</a> Ready	Tue, 24 Nov 2020 13:07:47 UTC Duration: 106.827 sec	B
6	<a href="https://104.26.13.49">104.26.13.49</a> Ready	Tue, 24 Nov 2020 13:09:34 UTC Duration: 109.174 sec	B

## Security Headers

The website failed the test with F. The website missed all the necessary security headers like; Strict-Transport-Security Content-Security-Policy X-Frame-Options X-Content-Type-Options Referrer-Policy Permissions-Policy. This implies that the website is susceptible to attacks like XSS, code injection, clickjacking.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.health.go.ug%2F&followRedirects=on>

The screenshot shows the Security Headers report for www.health.go.ug. The report is sponsored by Probely and shows a failing grade of F. The report includes a 'Scan your site now' button and a 'Security Report Summary' section with the following details:

**Security Report Summary**

- Site: <https://www.health.go.ug/>
- IP Address: 2606:4700:20:0:ac43:4768
- Report Time: 25 Nov 2020 07:38:05 UTC
- Headers:
  - ✗ Strict-Transport-Security
  - ✗ Content-Security-Policy
  - ✗ X-Frame-Options
  - ✗ X-Content-Type-Options
  - ✗ Referrer-Policy
  - ✗ Permissions-Policy

### 3. Blacklight

This application detected trackers on this page sending data to companies involved in online advertising. Blacklight detected scripts belonging to the companies Facebook, Inc., Twitter, Inc. and Alphabet, Inc. Blacklight also detected 4 third-party cookies on this site, this included cookies set for Stripe, Inc and Alphabet, Inc.

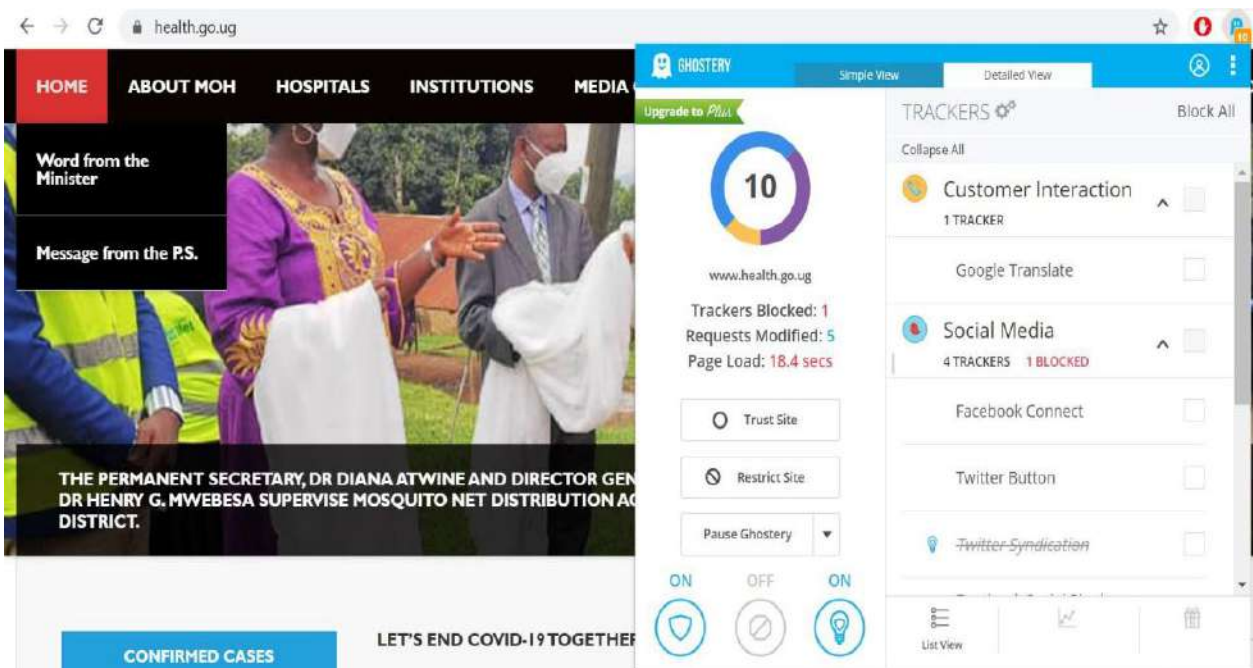
Canvas fingerprinting was detected on this website. This technique is designed to identify users even if they block third-party cookies. It can be used to track users' behavior across sites.

<https://themarkup.org/blacklight?url=www.health.go.ug>

<https://www.andreafortuna.org/2017/11/06/what-is-canvas-fingerprinting-and-how-the-companies-use-it-to-track-you-online/#:~:text=Canvas%20fingerprinting%20is%20a%20type,cookies%20or%20other%20similar%20means.>

### 4. Ghostery

The extension identified 10 trackers on the ministry of health website. These included; Facebook Connect, Google and Twitter trackers.



### 5. MyIP.is

According to the analysis done by MyIP, the website is hosted in San Francisco, USA.

<https://myip.ms/info/whois/104.26.12.49/k/774359933/website/www.health.go.ug>

# NIRA, Uganda

Officially NIRA doesn't have a mobile application. In this section we tested the official website of the organization (<https://www.nira.go.ug/>).

**SSL Lab Server Test:** The SSL server of NIRA's website scored a B. The website connection is encrypted with Transport Layer Security 1.2 (not the latest version). <https://www.ssllabs.com/ssltest/analyze.html?d=www.nira.go.ug>



**2. Security Headers:** The website was ranked with a B. It had two missing security headers namely; Content-security-policy and permissions-policy. This infers that the website is vulnerable to cross-site scripting and other injection attacks. <https://securityheaders.com/?q=https%3A%2F%2Fwww.nira.go.ug%2F&followRedirects=on>



**3. Blacklight Markup :** Blacklight detected a tracker on this page sending data to companies involved in online advertising. Blacklight detected a script belonging to the company Twitter, Inc.

**4. MyIp.is:** The website is hosted on a server located in Kampala, Uganda; according to the report by myip.is <https://themarkup.org/blacklight?url=www.nira.go.ug>



# Uganda Revenue Authority.

We carried out a test on URA's android mobile application (AskURA) and the official website.

**Mobile Application:** We used Exodus to check if the application has trackers. Only one tracker (Google AdMob) was identified. <https://reports.exodus-privacy.eu.org/en/reports/154783/>

**1 tracker**      **13 permissions**

Version 16 - [see other versions](#)  
 Source: Google Play  
 Report created on Nov. 25, 2020, 1:06 p.m.

[See on Google Play >](#)

**1 tracker**  
 We have found **code signature** of the following tracker in the application:  
 Google AdMob >  
 advertisement

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

**13 permissions**  
 We have found the following permissions in the application:

**2. Website:** The website is encrypted with the latest TLS version (1.3). Two cookies were recognized on the website. We used the following tools to analyze the website furthermore;

**SSL Lab Server test:** The SSL server of NIRA's website scored a B when it was analyzed by Qualys' SSL server test tool, this is because of its weakness in protocol support. <https://www.ssllabs.com/ssltest/analyze.html?d=www.ura.go.ug>

**SSL Report: www.ura.go.ug (196.10.228.59)**

Assessed on: Wed, 25 Nov 2020 13:35:07 UTC | [Hide](#) | [Clear cache](#)      [Scan Another »](#)

**Summary**

Overall Rating: **B**

Category	Score
Certificate	100
Protocol Support	70
Key Exchange	90
Cipher Strength	90

- Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).
- This server's certificate chain is incomplete. Grade capped to B.
- This server supports TLS 1.1. Grade capped to B. [MORE INFO »](#)
- This server supports TLS 1.3.
- HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

**b. Security Headers:** The website scored a D because lacked some security headers like Content Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. The website may be prone to attacks like cross-site scripting, Clickjacking, spoofing and others. <https://securityheaders.com/?q=https%3A%2F%2Fwww.ura.go.ug%2F&followRedirects=on>



### Security Report Summary

	Site:	<a href="https://www.ura.go.ug/">https://www.ura.go.ug/</a>
	IP Address:	196.10.228.59
	Report Time:	25 Nov 2020 12:49:02 UTC
	Headers:	<span>✔ Strict-Transport-Security</span> <span>✘ Content-Security-Policy</span> <span>✘ X-Frame-Options</span> <span>✘ X-Content-Type-Options</span> <span>✘ Referrer-Policy</span> <span>✘ Permissions-Policy</span>

**c. Blacklight Markup:** Blacklight detected trackers on this page sending data to companies involved in online advertising. The web app detected scripts belonging to the companies Twitter, Inc. and Alphabet, Inc.

**d. MyIP.is:** The servers that host the website are located at Nakawa Industrial Area, Kampala, Uganda. <https://themarkup.org/blacklight?url=www.ura.go.ug>

# Directorate of Citizenship and Immigration, Uganda.

In this section, we analyzed the website of the directorate of Citizenship and Immigration (<https://immigration.go.ug/>) and assessed its security level using the following web application tools;

**SSL Lab Server Test:** The SSL server of the website runs the latest Transport Layer Security version (1.3), it scored A after the analysis.

**Security Headers:** The website notched a D after the test, this because it had missing security headers like Content Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. The website may be prone to attacks like cross-site scripting, Clickjacking, spoofing and others.

<https://www.ssllabs.com/ssltest/analyze.html?d=immigration.go.ug> and <https://securityheaders.com/?q=https%3A%2F%2Fimmigration.go.ug%2F&followRedirects=on>



**c. Blacklight Markup:** Blacklight detected a script belonging to the company Facebook, Inc.

**d. MyIP:** Jurisdictions: The website is hosted on a server in Kampala, Uganda. <https://themarkup.org/blacklight?url=immigration.go.ug>



# 3. Insurance services app assessment

# UAP Insurance

**Mobile Application:** Apparently, we couldn't find a mobile application of UAP on Google's play store.

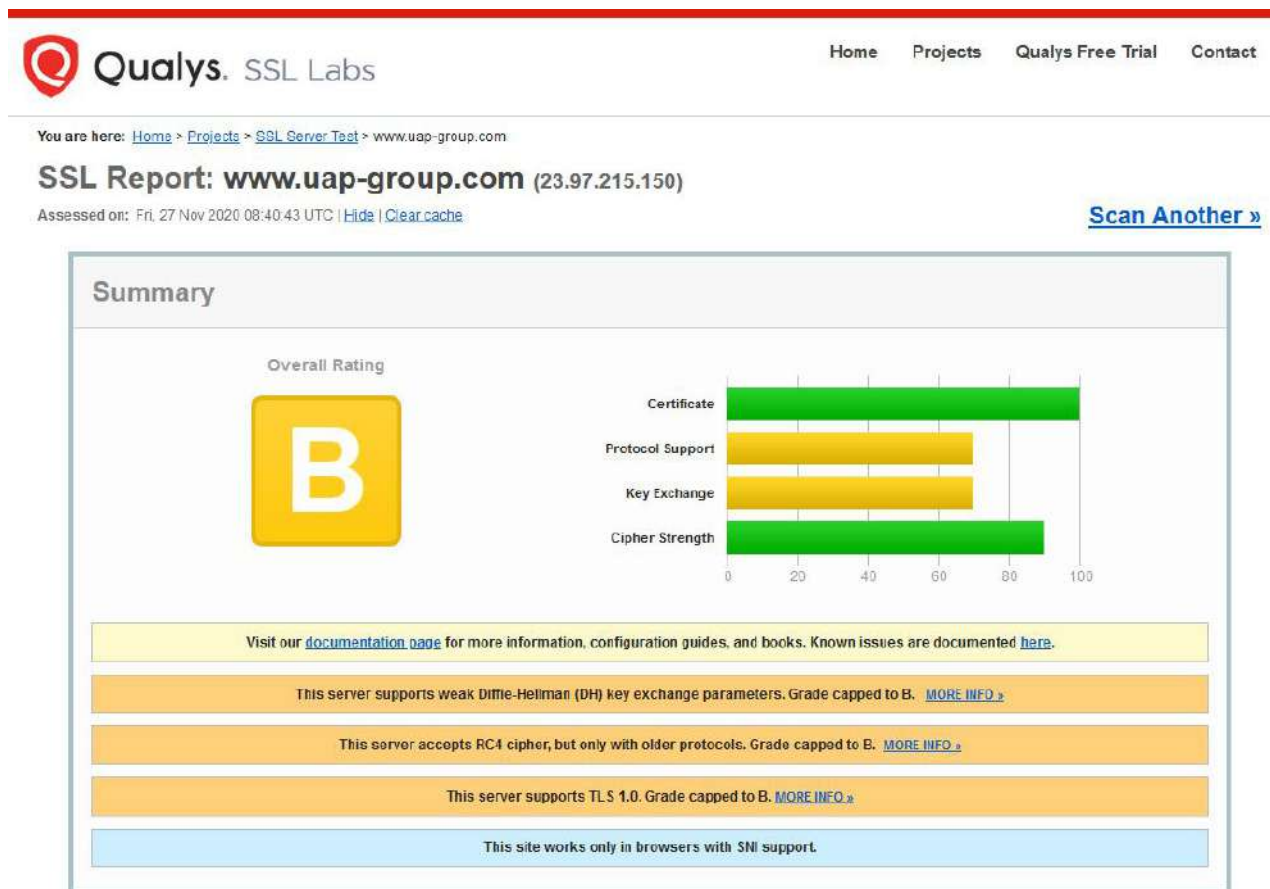
## Website

The website uses the RSA encryption standard with SHA-256 keys and TLS 1.2 to secure the website.

### a. SSL Lab Server Test

When we submitted in the domain of UAP, the server scored a B. The SSL server of UAP's website supports weak Diffie-Hellman (DH) key exchange parameters. The server also accepts RC4 cipher, but only with older protocols. It supports 1.1 and 1.2 TLS versions.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.uap-group.com>



**b. Security Headers:** The website missed the following security headers; Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, and Permissions-Policy.

**c. Blacklight Markup:** No trackers were identified on the website.

**d. MyIp:** The website is hosted on a Microsoft server in Washington, USA

<https://securityheaders.com/?q=https%3A%2F%2Fwww.uap-group.com%2Fsites%2Fuganda%2FPages%2FHome.aspx&followRedirects=on>

<https://myip.ms/info/whois/23.97.215.150/k/187553696/website/www.uap-group.com>

# SANLAM

**Mobile Application:** Only one tracker (Google Crashlytics) was identified by Exodus Privacy during the static analysis. <https://reports.exodus-privacy.eu.org/en/reports/154991/>

exodus Home Reports Trackers Better understand The organization en

Sanlam

**1** tracker **4** permissions

Version 2.6.202011171136\_live - [see other versions](#)  
Source: Google Play  
Report created on Nov. 27, 2020, noon

[See on Google Play >](#)

## Website

By the time of the analysis, the website was using a RSA encryption standard with AES 256 keys. We used the following tool to assess the security of the SSL server, certificate and find out the jurisdictions of the hosting server;

## SSL Lab Test Server by Qualys

The SSL server of the website failed the test. This is because it supports 512-bit export suites and might be vulnerable to the FREAK attack. A FREAK attack allows malicious players to intercept HTTPS connections between vulnerable clients and servers and force them to use 'export-grade' cryptography. This export-grade cryptography includes out-of-date encryption key lengths that can then easily be decrypted.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.sanlam.com>

Qualys. SSL Labs Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.sanlam.com](#)

**SSL Report: www.sanlam.com (196.36.206.27)**

Assessed on: Fri, 27 Nov 2020 12:00:18 UTC | [Hide](#) | [Clear cache](#) [Scan Another »](#)

**Summary**

Overall Rating

**F**

Category	Score
Certificate	100
Protocol Support	100
Key Exchange	100
Cipher Strength	100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

The SSL server supports insecure cipher suites as shown in the image below;

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	WEAK	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 2048 bits FS	WEAK	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		WEAK	112
TLS_RSA_WITH_RC4_128_SHA (0x5)		INSECURE	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)		INSECURE	128
TLS_RSA_WITH_DES_CBC_SHA (0x9)		INSECURE	56
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x64)		INSECURE	56
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3)		INSECURE	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8)		INSECURE	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6)		INSECURE	40
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15)	DH 2048 bits FS	INSECURE	56
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5 (0x60)		INSECURE	56
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 (0x61)		INSECURE	56

**Security Headers:** The website scored a D because it missed the following security headers; Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, and Permissions-Policy. This puts it at a risk of XSS attack.



### Security Report Summary

D

Site:	<a href="https://www.uap-group.com/sites/uganda/Pages/Home.aspx">https://www.uap-group.com/sites/uganda/Pages/Home.aspx</a>
IP Address:	23.97.215.150
Report Time:	27 Nov 2020 08:37:56 UTC
Headers:	<span style="color: green;">✔ X-Frame-Options</span> <span style="color: green;">✔ X-Content-Type-Options</span> <span style="color: red;">✘ Strict-Transport-Security</span> <span style="color: red;">✘ Content-Security-Policy</span> <span style="color: red;">✘ Referrer-Policy</span> <span style="color: red;">✘ Permissions-Policy</span>

**2. Blacklight Markup:** Two trackers and two cookies were detected on the website sending data to companies involved in online advertising. Blacklight detected a script belonging to the company Alphabet, Inc. (Google)

**3. MyIPs:** The server hosting Sanlam’s website is located in Johannesburg, South Africa.

<https://themarkup.org/blacklight?url=www.sanlam.com>

<https://myip.ms/info/whois/196.36.206.27/k/2917117712/website/www.sanlam.com>

# BRITAM

**Mobile Application:** Three trackers were identified during the static analysis by Exodus Privacy, namely; Google Analytics, Cordova, and Google Tag Manager.

<https://reports.exodus-privacy.eu.org/en/reports/155018/>

The screenshot shows the Exodus Privacy report for the Britam mobile application. The header includes the Exodus logo and navigation links: Home, Reports, Trackers, Better understand, and The organization. The main content area displays the Britam logo and key findings: 3 trackers and 7 permissions. It provides details such as Version 3.0.5, Source: Google Play, and Report created on Nov. 27, 2020, 3:28 p.m. A link to 'See on Google Play' is also present. Below this, a section titled '3 trackers' lists the following trackers found in the application: Google Analytics, Google Analytics Plugin (Cordova), and Google Tag Manager. A note explains that a tracker is software used to collect data about user usage, with a link to 'Learn more...'.

**Website:** The website is secured with TLS 1.2 and it's verified by Digi Cert Inc. It also uses RSA encryption standard with AES 256 keys.

**SSL Lab Server Test:** The SSL server of the website supported weak Diffie-Hellman (DH) key exchange parameters and TLS 1.1. Grade was capped to B.

<https://www.ssllabs.com/ssltest/analyze.html?d=ug.britam.com>

The screenshot shows the Qualys SSL Labs report for the website ug.britam.com. The header includes the Qualys SSL Labs logo and navigation links: Home, Projects, Qualys Free Trial, and Contact. The breadcrumb trail reads: You are here: Home > Projects > SSL Server Test > ug.britam.com. The main heading is 'SSL Report: ug.britam.com (196.41.68.19)'. Below this, it states 'Assessed on: Fri, 27 Nov 2020 15:32:32 UTC' with links to 'Hide' and 'Clear cache'. A 'Scan Another »' button is also visible. The 'Summary' section features a large yellow box with the letter 'B' representing the Overall Rating. To the right, a horizontal bar chart shows the scores for different SSL/TLS components: Certificate (100%), Protocol Support (70%), Key Exchange (70%), and Cipher Strength (90%).




## Security Headers

The website scored a D didn't have the following security headers; Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, and Permissions-Policy.

<https://securityheaders.com/?q=https%3A%2F%2Fug.britam.com%2F&followRedirects=on>



Security Report Summary	
	Site: <a href="https://ug.britam.com/">https://ug.britam.com/</a>
	IP Address: 196.41.68.19
	Report Time: 27 Nov 2020 15:28:45 UTC
	Headers: <ul style="list-style-type: none"> <li>✔ X-Frame-Options</li> <li>✔ X-Content-Type-Options</li> <li>✘ Strict-Transport-Security</li> <li>✘ Content-Security-Policy</li> <li>✘ Referrer-Policy</li> <li>✘ Permissions-Policy</li> </ul>

## 2. Blacklight Markup

Blacklight detected Alphabet Inc's trackers on the website sending data to companies involved in online advertising.

## 3. Mylp

It's hosted in Nairobi, Kenya. <https://themarkup.org/blacklight?url=ug.britam.com>

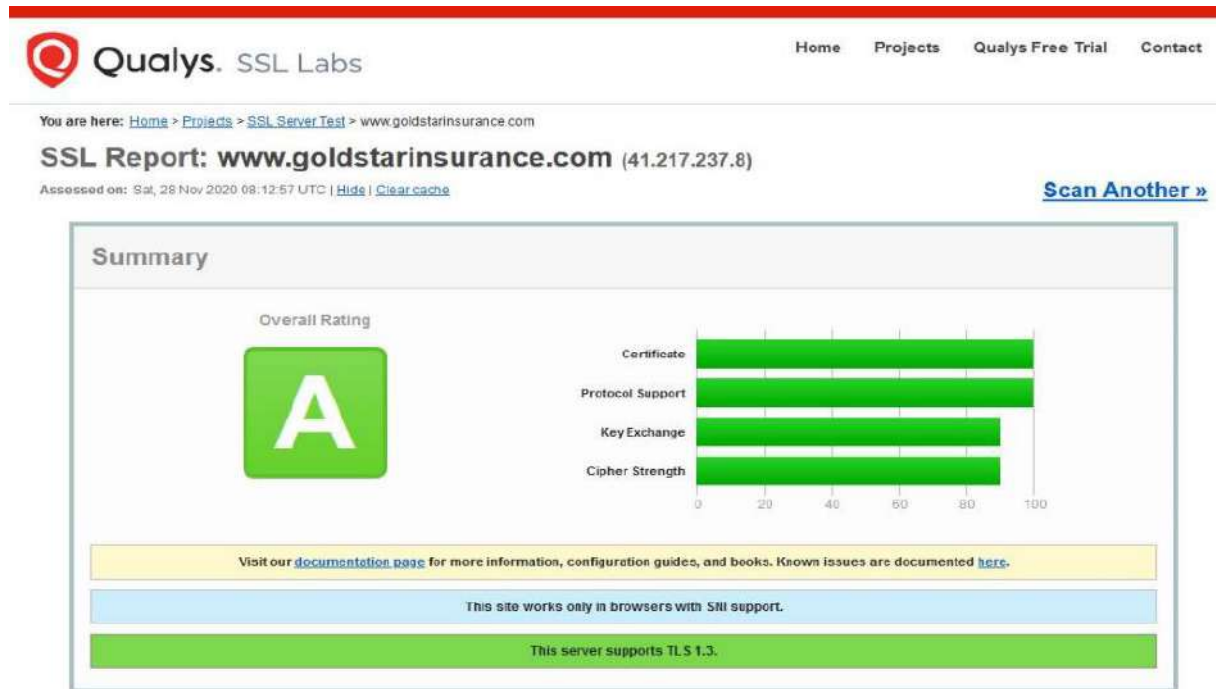
# GOLDSTAR

**Mobile Application:** The company didn't have a mobile app in place by the time we carried out this analysis.

**Website:** The company coupled the latest version of the transport layer security (1.3) together with AES encryption to secure the website. We used the following tools to analyze the website further;

**SSL Server Lab Test:** The SSL server of Goldstar's website scored A after the test. According to the test report, the server showed security strength in both the SSL certificate and protocol support.

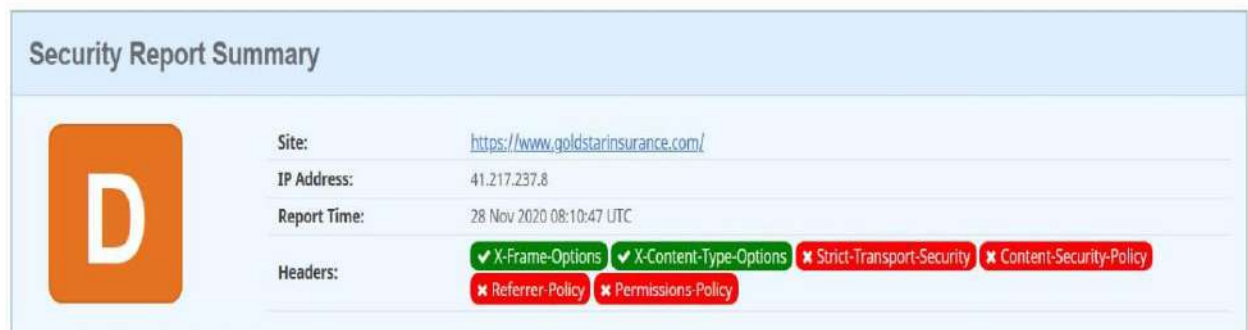
<https://www.ssllabs.com/ssltest/analyze.html?d=www.goldstarinsurance.com>



## 2. Security Headers

According to the report by security headers, the website scored a D because it lacks some security headers as shown below;

<https://securityheaders.com/?q=https%3A%2F%2Fwww.goldstarinsurance.com%2F&followRedirects=on>



### 3. Blacklight Markup

This tool detected a script belonging to the company Alphabet, Inc. (Google). According to Blacklight, the website uses Google Analytics and seems to use its "remarketing audiences" feature that enables user tracking for targeted advertising across the internet. This feature allows a website to build custom audiences based on how a user interacts with this particular site and then follow those users across the internet and target them with advertising.

### 4. MyIP

According to Myip.ms findings, the server hosting the website is situated in Kampala, Uganda.

<https://themarkup.org/blacklight?url=www.goldstarinsurance.com>

<https://myip.ms/info/whois/41.217.237.8/k/295439408/website/www.goldstarinsurance.com>

# JUBILEE INSURANCE

## Mobile Application

The company didn't have a mobile application to deliver services to Ugandans by the time we carried out this analysis.

## Website

The company employed version 1.2 of the transport layer security together with advanced encryption standard of 128 keys. We analyzed the security of the SSL server, and the certificate using the following tools;

## SSL Server Lab Test

Since the server supported the older versions of TLS, the grade was capped to B.

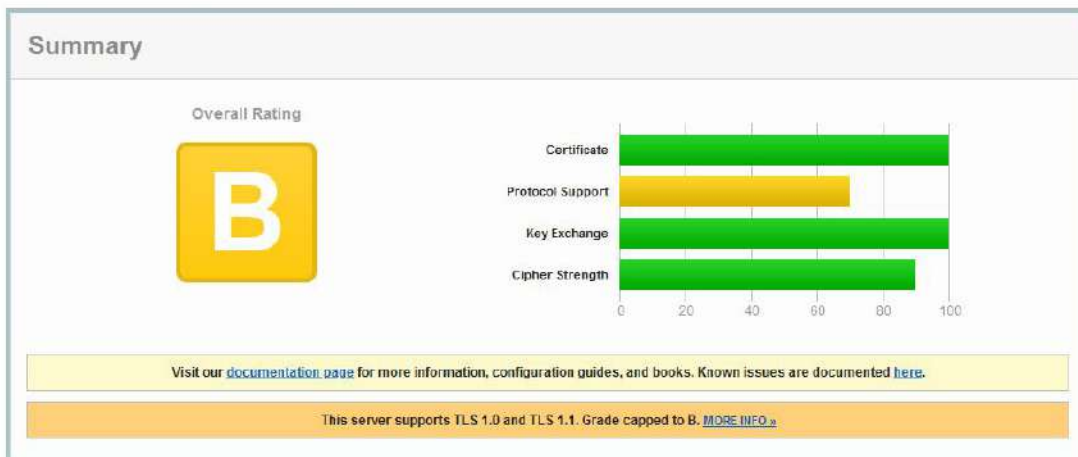
<https://www.ssllabs.com/ssllabs/analyze.html?d=www.jubileeinsurance.com>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.jubileeinsurance.com](#)

### SSL Report: [www.jubileeinsurance.com](#) (18.134.130.29)

Assessed on: Sat, 28 Nov 2020 08:41:33 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



## 2. Security Headers

The website failed the test with F. According to the report by Security Headers website, the website had none of the essential security headers. This makes it susceptible to attacks like cross-site scripting.

The image shows a 'Security Report Summary' for the website <https://www.jubileeinsurance.com/ug/>. The report indicates a failed grade of 'F'. The IP address is 18.134.130.29 and the report was generated on 28 Nov 2020 at 08:39:56 UTC. Under the 'Headers' section, several essential security headers are listed as missing: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy.

Field	Value
Site:	<a href="https://www.jubileeinsurance.com/ug/">https://www.jubileeinsurance.com/ug/</a>
IP Address:	18.134.130.29
Report Time:	28 Nov 2020 08:39:56 UTC
Headers:	✘ Strict-Transport-Security ✘ Content-Security-Policy ✘ X-Frame-Options ✘ X-Content-Type-Options ✘ Referrer-Policy ✘ Permissions-Policy

## 3. Blacklight Markup

No tracker was detected on Jubilee's website.

## 4. MyIPs

The website is hosted in Cambridge, Massachusetts, USA

<https://myip.ms/info/whois/18.134.130.29/k/2064803358/website/www.jubileeinsurance.com>

# Statewide Insurance (SWICO)

**Mobile Application:** The company didn't have a mobile application by the time we carried out this analysis.

**Website:** The connection to the website was secured with a SSL certificate verified by Let's Encrypt and ran TLS 1.3.

**SSL Server Lab Test:** The SSL Server scored a B after the analysis. This is because the server supports forward secrecy making it vulnerable to ROBOT attacks. The ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability allows anyone on the Internet to perform RSA decryption and signing operations with the private key of a TLS server.

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/robot-attack-detected-strong-oracle/>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.swico.co.ug](#)

**SSL Report: www.swico.co.ug (158.85.53.149)**

Assessed on: Sat 28 Nov 2020 09:03:13 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



**2. Security Headers:** According to the findings of securityheaders.io, the website failed the test because it didn't have the essential security headers in place to mitigate cyber-attacks like cross-site scripting.



**3. Blacklight Markup:** Blacklight detected two trackers belonging to the company Alphabet, Inc. (Google)

**4. MyIP:** It's hosted in Virginia, USA.

<https://themarkup.org/blacklight?url=www.swico.co.ug> and <https://myip.ms/info/whois/158.85.53.149/k/1120899812/website/www.swico.co.ug>

# ICEA Lion

## Mobile Application

We analyzed the company's mobile android application using Exodus Privacy tool. No tracker was identified in the application during the static analysis.

**0 trackers**      **18 permissions**

Version 1.3 - [see other versions](#)  
Source: [Google Play](#)  
Report created on Nov. 23, 2020, 9:19 a.m.

[See on Google Play >](#)

**0 trackers**

We have not found **code signature** of any tracker we know in the application. The application could contain tracker(s) we do not know yet.

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

## Website

The connection to this website is encrypted with TLS 1.2 and SHA256 with RSA.

### SSL Server Lab Test

According to Qualys' Server Test, the SSL server scored A.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.icealion.com>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.icealion.com](#)

### SSL Report: [www.icealion.com](#) (160.153.141.139)

Assessed on: Sat, 28 Nov 2020 09:23:24 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

**Summary**

Overall Rating

**A**

Category	Score
Certificate	100
Protocol Support	100
Key Exchange	100
Cipher Strength	100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP request to this server failed, see [below](#) for details.

This site works only in browsers with SNI support.

## 2. Security Headers

Overall, the website scored a C because it had missing security headers.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.icealion.com%2F&followRedirects=on>

### Security Report Summary

C

Site:	<a href="https://www.icealion.com/">https://www.icealion.com/</a>
IP Address:	160.153.141.139
Report Time:	28 Nov 2020 09:20:25 UTC
Headers:	<div style="display: flex; gap: 5px;"> <div style="background-color: #27ae60; color: white; padding: 2px 5px; border-radius: 3px;">✔ X-Frame-Options</div> <div style="background-color: #27ae60; color: white; padding: 2px 5px; border-radius: 3px;">✔ X-Content-Type-Options</div> <div style="background-color: #27ae60; color: white; padding: 2px 5px; border-radius: 3px;">✔ Referrer-Policy</div> <div style="background-color: #e74c3c; color: white; padding: 2px 5px; border-radius: 3px;">✘ Strict-Transport-Security</div> <div style="background-color: #e74c3c; color: white; padding: 2px 5px; border-radius: 3px;">✘ Content-Security-Policy</div> <div style="background-color: #e74c3c; color: white; padding: 2px 5px; border-radius: 3px;">✘ Permissions-Policy</div> </div>

## 3. Blacklight Markup

Blacklight detected three trackers on the website sending data to companies involved in online anamely; Facebook, Inc. and Alphabet, Inc. (Google). Furthermore, Blacklight also detected Facebook Pixel on ICEA's website. The Facebook pixel is a snippet of code that sends data back to Facebook about people who visit this site and allows the site operator to later target them with ads on Facebook.

## 4. MyIP

The website is hosted on a server in Arizona, USA according to this report.

<https://themarkup.org/blacklight?url=www.icealion.com>

<https://myip.ms/info/whois/160.153.141.139/k/688971764/website/www.icealion.com>

# 4. Private Hospital app assessment



# Case Hospital

## Mobile Application

We couldn't find any android application of Case Clinic on Google's Play Store.

## Website (casemedcare.org)

The company employs TLS 1.3 with AES algorithm with 256 bit keys to encrypt the connection and data on the website.

## SSL Lab Server Test

The SSL Server of the website scored A after the test.

<https://www.ssllabs.com/ssltest/analyze.html?d=casemedcare.org>

### SSL Report: casemedcare.org (8.29.157.92)

Assessed on: Mon, 30 Nov 2020 09:13:23 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



## b. Security Headers

According to the analysis report by securityheaders.io, the website failed the test because it didn't have all the essential security headers. These leaves it susceptible to cyber-attacks like click-jacking and injection attacks.

<https://securityheaders.com/?q=https%3A%2F%2Fcasemedcare.org%2F&followRedirects=on>



## c. Blacklight Markup

No third-party trackers or cookies were detected on the website.

## d. MyIp

The website was hosted in Ohio State, USA by the time this analysis was executed.

# International Hospital Kampala (IHK)

No android application belonging to IHK was identified on Google's PlayStore.

**Website (ihk.img.co.ug/):** The company uses TLS 1.3 with AES algorithm with 256 bit keys to encrypt the website connections. The SSL certificate is verified by 'Let's Encrypt'

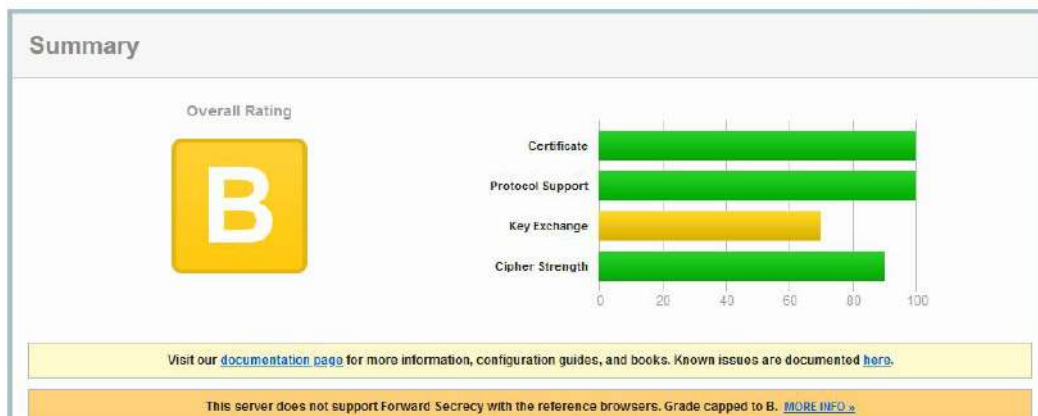
**SSL Lab Server Test:** According to the analysis report by Qualys' tool, the SSL server scored a B because it didn't support forward secrecy with the reference browsers.

<https://www.ssllabs.com/ssltest/analyze.html?d=ihk.img.co.ug>

## SSL Report: [ihk.img.co.ug](https://www.ssllabs.com/ssltest/analyze.html?d=ihk.img.co.ug) (50.22.208.143)

Assessed on: Mon, 30 Nov 2020 09:37:01 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



**b. Security Headers:** The website failed the test because it lacked all the essential security headers.

<https://securityheaders.com/?q=https%3A%2F%2Fihk.img.co.ug%2F&followRedirects=on>



**c. Blacklight Markup**

Three ad trackers owned by Alphabet Inc. (Google) and Facebook were identified on this website. Websites containing advertising tracking technology load Javascript code or small invisible images that are used to either build your advertising profile or to identify you for ad targeting on the internet. More so, the website uses the Facebook Pixel feature to send data back to Facebook.

<https://themarkup.org/blacklight?url=ihk.img.co.ug>

**d. MyIp**

The website is hosted in the state of Virginia, USA.

<https://myip.ms/info/whois/50.22.208.143/k/748939688/website/ihk.img.co.ug>

# Nakasero Hospital

**Mobile App:** No mobile application affiliated to Nakasero Hospital was found on Google’s PlayStore.

**Website (<http://nakaserohospital.com>):** The website lacked a SSL certificate by the time we carried out this research.

**SSL Lab Server Test:** The SSL certificate of the website wasn’t trustful according to the report by SSL Lab. This is because it expired on 29th June, 2018.

<https://www.ssllabs.com/ssltest/analyze.html?d=nakaserohospital.com>

## SSL Report: nakaserohospital.com (160.153.47.1)

Assessed on: Mon, 30 Nov 2020 10:35:46 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



### b. Security Headers

The website scored an E because it had only one of the essential security headers.

<https://securityheaders.com/?q=http%3A%2F%2Fnakaserohospital.com%2F&followRedirects=on>



### c. Blacklight Markup

Blacklight detected a script of an ad-tracker belonging to the company Facebook, Inc.

### d. MyIp

The website is hosted by GoDaddy in the state of Arizona, USA.

<https://themarkup.org/blacklight?url=nakaserohospital.com>

<https://myip.ms/info/whois/160.153.47.1/k/2375897079/website/nakaserohospital.com>

# Paragon Hospital

## Mobile App

Paragon hospital didn't have an android mobile app by the time we carried out this research.

## Website (paragonhospital.ug)

The website is partially encrypted; parts of the website were not encrypted before being transmitted. This means that the information sent over the internet using this website can be viewed in transit.

## SSL Lab Server Test

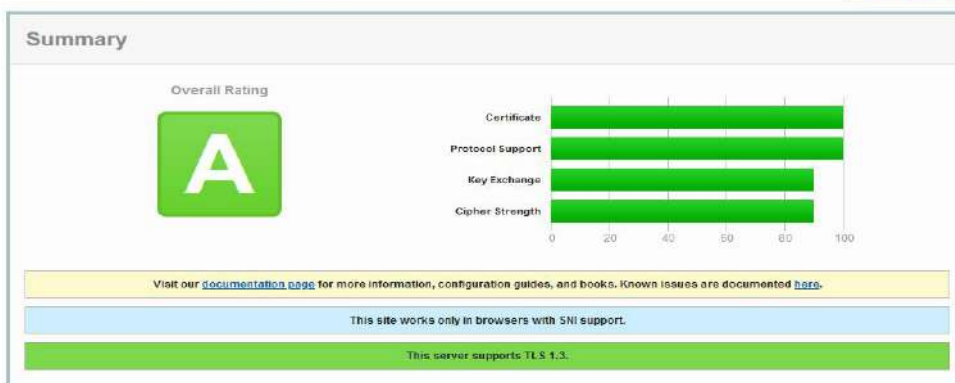
Using Qualys' SSL server test to assess the security of the SSL server of the hospital's website, the server scored A

<https://www.ssllabs.com/ssltest/analyze.html?d=paragonhospital.ug>

### SSL Report: paragonhospital.ug (67.205.177.204)

Assessed on: Mon, 30 Nov 2020 10:55:19 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)



## b. Security Headers

The website failed the test by securityheaders.io with F. This is because it lacked or the required security headers

<https://securityheaders.com/?q=https%3A%2F%2Fparagonhospital.ug%2F&followRedirects=on>



## c. Blacklight Markup

Only one ad-tracker belonging to Alphabet, Inc. was detected on the website.

## d. MyIp

According to the report by myip.ms, the website is hosted on a server in New York, USA.

# MTN-Uganda

## Mobile Apps

Exodus Privacy

### MyMTN

The Exodus Privacy Tool analyzed and identified two Google trackers that is; Google Crashlytics and Google Firebase, the application also requires 15 permissions on 20th November, 2020.

exodus v1.20



## MyMTN

**2 trackers** **15 permissions**

Version 3.0.1 - [see other versions](#)  
 Source: Google Play  
 Report created on Oct. 5, 2020, 2:20 p.m. and updated on Oct. 7, 2020, 2:09 p.m.  
[See on Google Play >](#)

**2 trackers**

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

- Google Crashlytics >  
[crash reporting](#)
- Google Firebase Analytics >  
[analytics](#)

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

**15 permissions**

We have found the following permissions in the application:

- ACCESS\_FINE\_LOCATION**  
access precise location (GPS and network-based)
- ACCESS\_NETWORK\_STATE**  
view network connections
- ACCESS\_WIFI\_STATE**  
view Wi-Fi connections

### b. MTN MoMo

According to the analysis that we carried out on 20th November, 2020; the application has one tracker and requires 14 permissions.



## MTN MoMo

**1 tracker** **14 permissions**

Version 1.0.1 - [see other versions](#)  
 Source: Google Play  
 Report created on June 9, 2020, 4:20 p.m. and updated on Oct. 7, 2020, 5:06 p.m.  
[See on Google Play >](#)

**1 tracker**

We have found **code signature** of the following tracker in the application:

- Google Analytics >  
[analytics](#)

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

**14 permissions**

We have found the following permissions in the application:

- ACCESS\_FINE\_LOCATION**  
access precise location (GPS and network-based)
- ACCESS\_NETWORK\_STATE**  
view network connections
- ACCESS\_WIFI\_STATE**  
view Wi-Fi connections
- CAMERA**  
take pictures and videos
- FLASHLIGHT**
- INTERNET**

## 2. Website

### Security Headers.

The SSL certificate of the domain <https://www.mtn.co.ug/> scored a C when it was analyzed by Security Headers. The SSL certificate missed the following headers;

Content-Security-Policy; Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

Referrer-Policy; Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

Permissions-Policy; Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

### MyIp

From the findings, MTN-Uganda hosts all of its users' data in Uganda.

<https://securityheaders.com/?q=https%3A%2F%2Fwww.mtn.co.ug%2F>

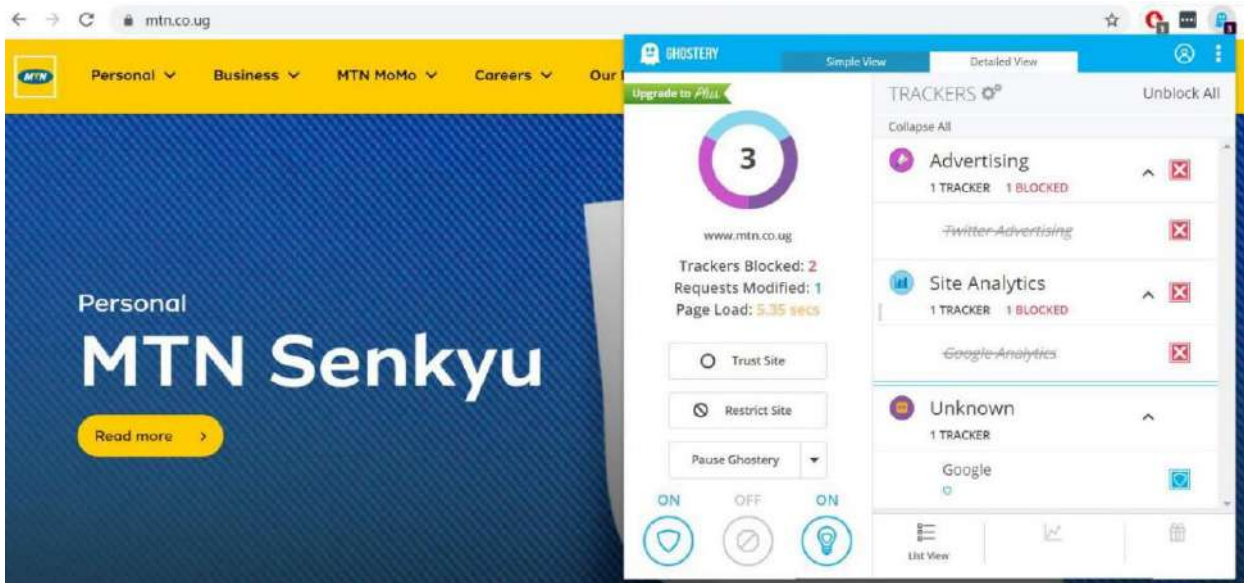
<https://myip.ms/info/whois/41.210.130.172/k/2237717804/website/www.mtn.co.ug>

Whois Web Hosting Information for website - [www.mtn.co.ug](http://www.mtn.co.ug) - 23 November 2020, 10:27:30

Hosting Info for Website:	<a href="http://www.mtn.co.ug">www.mtn.co.ug</a>	#91,125 position in world sites rating
Popularity:	5,630 visitors per day	Hide Map »
IP Address:	<a href="http://41.210.130.172">41.210.130.172</a>	
IP Location:	Uganda, Central Region, Kampala	
IP Reverse DNS (Host):	<a href="http://h2ac.n1.ips.mtn.co.ug">h2ac.n1.ips.mtn.co.ug</a>	
Top Level Host Usage:	9 sites use XXX.mtn.co.ug as IP Reverse DNS	
Hosting Company / IP Owner:	Mtn Uganda	
Owner IP Range:	<a href="http://41.210.128.0">41.210.128.0</a> - <a href="http://41.210.191.255">41.210.191.255</a> (16,384 ip) <a href="#">Other Sites on IP »</a>	
Owner Address:	7/F, Eastern Plaza, Plot 59A, Yusuf Lule Road, P.o.box 24624, Kampala	
Owner Country:	Uganda	
Owner Phone:	+256 312 120111, tel:+256-31-2120111	
Owner Website:	<a href="http://www.mambosms.ug">www.mambosms.ug</a>	
Owner CIDR:	<a href="http://41.210.128.0/18">41.210.128.0/18</a>	

**c. Blacklight**

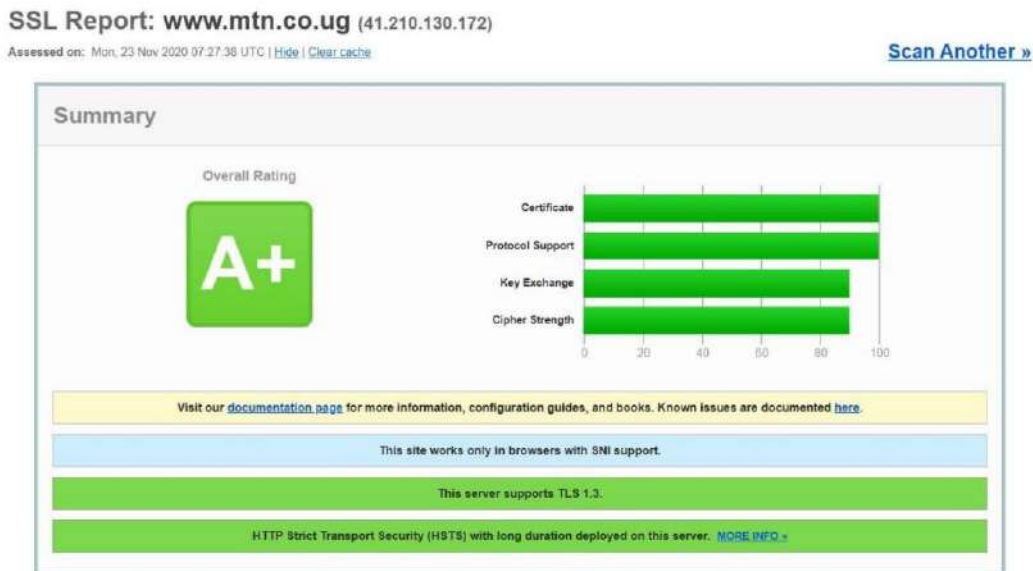
Blacklight detected trackers on this page sending data to companies involved in online advertising. Blacklight detected scripts belonging to the companies Alphabet, Inc. and Twitter, Inc.



**d. SSL Labs.**

The website SSL scored A+ after it was analyzed by SSL labs.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.mtn.co.ug>



# Airtel Uganda

## Mobile Applications

Exodus Privacy Tool

### My Airtel

The Exodus tool found code signatures of the following trackers; Apps Flyer, Google Firebase Analytics, and Google Crashlytics.

<https://reports.exodus-privacy.eu.org/en/reports/154595/>

The screenshot shows the Exodus Privacy Tool interface for the application 'My Airtel'. At the top, there is a navigation bar with the Exodus logo and links for Home, Reports, Trackers, Better understand, and The organization. The main content area features the Airtel logo and the application name 'My Airtel'. Below this, two statistics are displayed: '3 trackers' and '29 permissions'. The report details include 'Version 1.2.2 - see other versions', 'Source: Google Play', and 'Report created on Nov. 23, 2020, 2:24 p.m.'. A link to 'See on Google Play' is provided. Under the '3 trackers' section, it lists 'code signature' of the following trackers: AppsFlyer (analytics), Google Crashlytics (crash reporting), and Google Firebase Analytics (analytics). A note explains that a tracker is software meant to collect data about the user or their usage, with a link to 'Learn more...'. The '29 permissions' section indicates that 29 permissions were found in the application.

### ii. Airtel TV

The tool couldn't download and decompile the application's apk.

<https://reports.exodus-privacy.eu.org/en/analysis/258400/>



## 2. Website (<https://www.airtel.co.ug/>)

### SSL lab.

The site scored A+ when it was assessed. The site had the latest TLS version.

### Security Headers

The website's SSL certificate scored a D after the assessment. The SSL certificate missed the following headers; Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy.

### Blacklight

Blacklight detected trackers on this website sending data to companies involved in online advertising. Blacklight detected scripts belonging to companies like Facebook, Inc., LinkedIn Corporation and Alphabet, Inc.

When you visit this website, it tells Facebook! The Facebook pixel is a snippet of code that sends data back to Facebook about people who visit this site and allows the site operator to later target them with ads on Facebook.

This website uses Google Analytics and seems to use its "remarketing audiences" feature that enables user tracking for targeted advertising across the internet.

### MyIp

According to the information collected from MyIP website, the website is hosted in Nairobi, Kenya.

### Ghostery

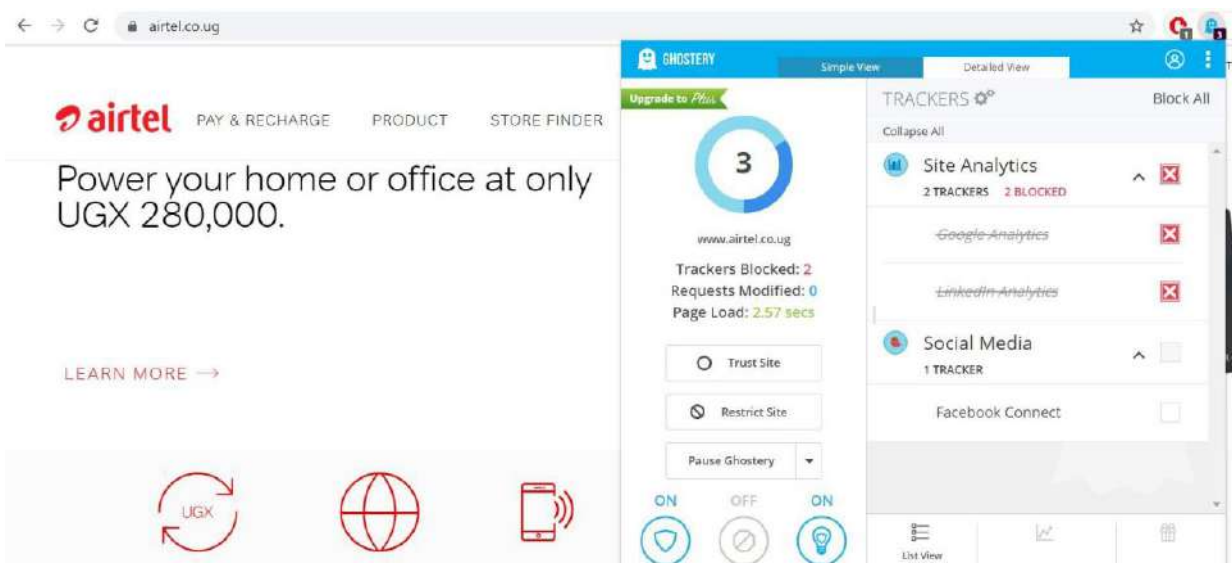
This extension tool identified three trackers namely; Google Analytics, LinkedIn Analytics and Facebook Connect.

<https://www.ssllabs.com/ssltest/analyze.html?d=www.airtel.co.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fwww.airtel.co.ug%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=www.airtel.co.ug>

<https://myip.ms/info/whois/41.223.58.200/k/3158352025/website/www.airtel.co.ug>



# Africell Uganda.

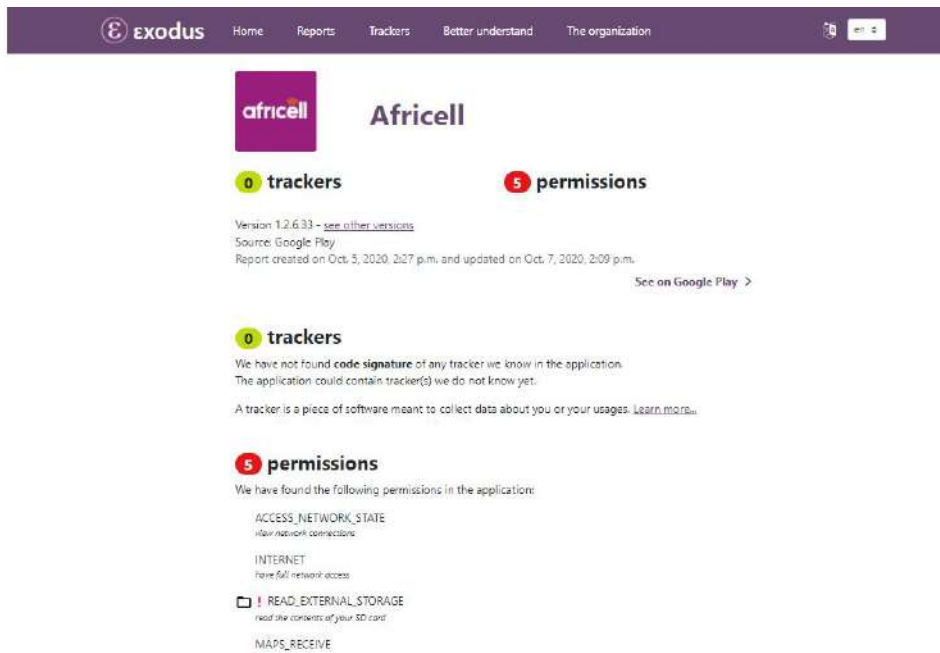
## Mobile Application

Exodus Privacy Tool.

On performing a new analysis on Africell’s mobile app using Exodus, no trackers where identified.

<https://play.google.com/store/apps/details?id=com.africell.africell.africellapp>

<https://reports.exodus-privacy.eu.org/en/reports/149855/>



## 2. Website.

NOTE: As of 24th November, 2020, the website was partially encrypted according to the security page info generated by Mozilla Firefox. Parts of the web-pages such as images were not encrypted.

### SSL Server Test

The website scored a B after the test.

### Security Headers

We got an error when we performed an analysis on the website.

“The target site took too long to respond and the connection timed out. Try again later.”

### Blacklight Markup

Blacklight did not detect any third-party user tracking technology present on this website. This can mean that this website is not tracking users.

### MyIP

According to MyIP, the website is hosted in Uganda.

<https://www.ssllabs.com/ssltest/analyze.html?d=africell.ug>

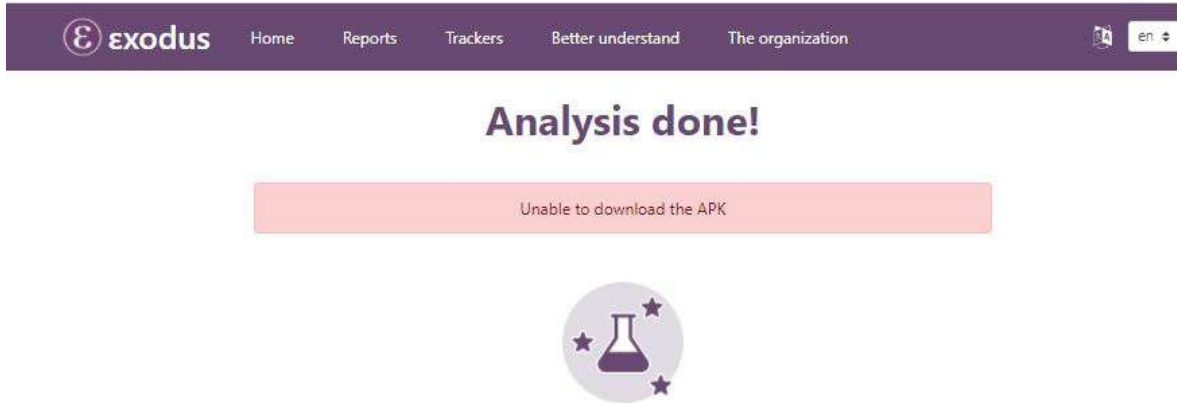
<https://securityheaders.com/?q=https%3A%2F%2Fafricell.ug%2F&followRedirects=on>

<https://myip.ms/info/whois/197.157.8.15/k/848301909/website/africell.ug>

# Uganda Telecom.

Mobile App (Msente)

Exodus Privacy tool couldn't download the application from the google play store.



## 2. Website (<https://www.utl.co.ug/>)

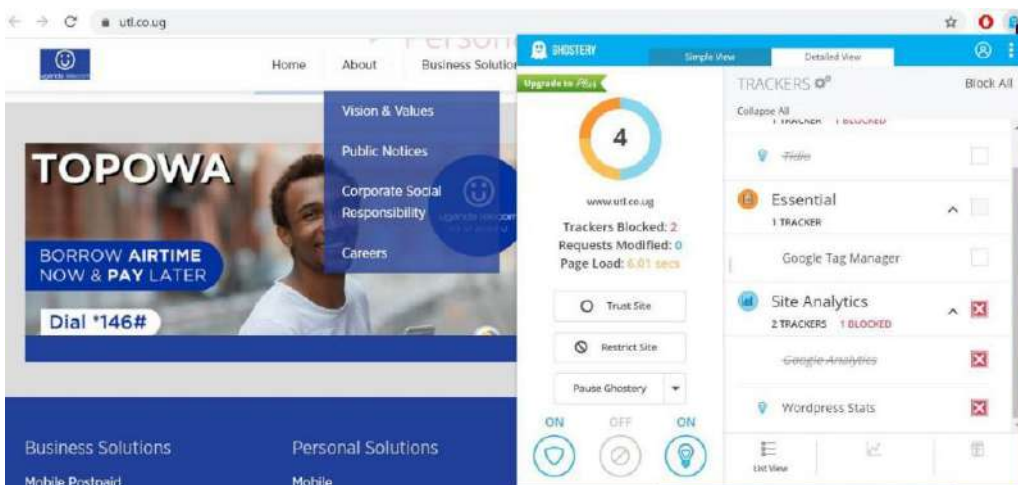
**a. SSL Lab Server Test:** This server accepts RC4 cipher, but only with older protocols. Grade capped to B.

**b. Security Headers:** Blacklight detected trackers on this page sending data to companies involved in online advertising. Blacklight detected a script belonging to the company Alphabet, Inc. These included; Google Analytics, Google Tag Manager.

**c. Ghostery:** The extension identified four trackers on UTL's website. These include; Tidio, Google Analytics, Google Tag Manager and WordPress stats.

<https://www.ssllabs.com/sslttest/analyze.html?d=www.utl.co.ug>

<https://themarkup.org/blacklight?url=www.utl.co.ug>



## d. MyIP

The company hosts it's website in Uganda according to MyIP.is website.

# References

- <https://www.thesslstore.com/blog/http-security-headers/>
- <https://reports.exodus-privacy.eu.org/en/reports/149849/>
- <https://www.unwantedwitness.org/download/uploads/Trading-Privacy.pdf>
- <https://www.ssllabs.com/ssltest/analyze.html?d=safeboda.com>
- <https://www.ssllabs.com/ssltest/analyze.html?d=safeboda.com>
- <https://community.qualys.com/blogs/securitylabs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack>
- <https://securityheaders.com/?q=https%3A%2F%2Fsafeboda.com%2Fug%2F&followRedirects=on>
- <https://securityheaders.com/?q=https%3A%2F%2Fsafeboda.com%2Fug%2F&followRedirects=on>
- <https://themarkup.org/blacklight?url=safeboda.com>
- <https://myip.ms/info/whois/188.166.152.84/k/1322050964/website/safeboda.com>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.Jumia.ug>
- [https://docs.google.com/spreadsheets/d/1E4avne1zl\\_FaMjO9FXilzwRYn4J8ldWJrKA3ds5vs3k/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1E4avne1zl_FaMjO9FXilzwRYn4J8ldWJrKA3ds5vs3k/edit?usp=sharing)
- [https://docs.google.com/spreadsheets/d/1t5QGTIBqHngQaBiYzsEzk\\_lseCh-oE1j0ufu6ksxcpA/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1t5QGTIBqHngQaBiYzsEzk_lseCh-oE1j0ufu6ksxcpA/edit?usp=sharing)
- <https://reports.exodus-privacy.eu.org/en/reports/149849/>
- <https://www.unwantedwitness.org/download/uploads/Trading-Privacy.pdf>
- <https://www.ssllabs.com/ssltest/analyze.html?d=safeboda.com>
- <https://community.qualys.com/blogs/securitylabs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack>
- <https://securityheaders.com/?q=https%3A%2F%2Fsafeboda.com%2Fug%2F&followRedirects=on>
- <https://themarkup.org/blacklight?url=safeboda.com>
- <https://myip.ms/info/whois/188.166.152.84/k/1322050964/website/safeboda.com>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.glovoapp.com>
- <https://themarkup.org/blacklight?url=glovoapp.com>
- <https://reports.exodus-privacy.eu.org/en/reports/154919/>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.stanbicbank.co.ug>
- <https://securityheaders.com/?q=https%3A%2F%2Fwww.stanbicbank.co.ug%2F&followRedirects=on>
- <https://themarkup.org/blacklight?url=www.stanbicbank.co.ug>
- <https://myip.ms/info/whois/104.16.86.99/k/3085277320/website/www.stanbicbank.co.ug>
- <https://mixpanel.com/behavioral-analytics/>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.sc.com>
- <https://securityheaders.com/?q=https%3A%2F%2Fwww.sc.com%2Fug%2F&followRedirects=on>
- <https://themarkup.org/blacklight?url=www.sc.com>
- <https://reports.exodus-privacy.eu.org/en/reports/154942/>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.centenarybank.co.ug>
- <https://themarkup.org/blacklight?url=www.centenarybank.co.ug>
- <https://www.ssllabs.com/ssltest/analyze.html?d=www.absa.co.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fwww.absa.co.ug%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=absa.co.ug>  
<https://reports.exodus-privacy.eu.org/en/reports/154982/>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.dfcugroup.com>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.dfcugroup.com%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=www.dfcugroup.com>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.health.go.ug>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.health.go.ug%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=www.health.go.ug>  
<https://www.andreafortuna.org/2017/11/06/what-is-canvas-fingerprinting-and-how-the-companies-use-it-to-track-you-online/#:~:text=Canvas%20fingerprinting%20is%20a%20type,cookies%20or%20other%20similar%20means.>  
<https://myip.ms/info/whois/104.26.12.49/k/774359933/website/www.health.go.ug>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.nira.go.ug>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.nira.go.ug%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=www.nira.go.ug>  
<https://reports.exodus-privacy.eu.org/en/reports/154783/>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.ura.go.ug>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.ura.go.ug%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=www.ura.go.ug>  
<https://www.ssllabs.com/ssltest/analyze.html?d=immigration.go.ug>  
<https://securityheaders.com/?q=https%3A%2F%2Fimmigration.go.ug%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=immigration.go.ug>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.uap->

[group.com](https://securityheaders.com/?q=https%3A%2F%2Fwww.uap-group.com%2Fsites%2Fuganda%2FPages%2FHome.aspx&followRedirects=on)  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.uap-group.com%2Fsites%2Fuganda%2FPages%2FHome.aspx&followRedirects=on>  
<https://myip.ms/info/whois/23.97.215.150/k/187553696/website/www.uap-group.com>  
<https://reports.exodus-privacy.eu.org/en/reports/154991/>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.sanlam.com>  
<https://themarkup.org/blacklight?url=www.sanlam.com>  
<https://myip.ms/info/whois/196.36.206.27/k/2917117712/website/www.sanlam.com>  
<https://reports.exodus-privacy.eu.org/en/reports/155018/>  
<https://www.ssllabs.com/ssltest/analyze.html?d=ug.britam.com>  
<https://securityheaders.com/?q=https%3A%2F%2Fug.britam.com%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=ug.britam.com>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.goldstarinsurance.com>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.goldstarinsurance.com%2F&followRedirects=on>  
<https://themarkup.org/blacklight?url=www.goldstarinsurance.com>  
<https://myip.ms/info/whois/41.217.237.8/k/295439408/website/www.goldstarinsurance.com>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.jubileinsurance.com>  
<https://myip.ms/info/whois/18.134.130.29/k/2064803358/website/www.jubileinsurance.com>  
<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/robot-attack-detected-strong-oracle/>  
<https://themarkup.org/blacklight?url=www.swico.co.ug>  
<https://myip.ms/info/whois/158.85.53.149/k/1120899812/website/www.swico.co.ug>  
<https://www.ssllabs.com/ssltest/analyze.html?d=www.icealion.com>  
<https://securityheaders.com/?q=https%3A%2F%2Fwww.icealion.com%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=www.icealion.com>

<https://myip.ms/info/whois/160.153.141.139/k/688971764/website/www.icealion.com>

<https://www.ssllabs.com/ssltest/analyze.html?d=casemedcare.org>

<https://securityheaders.com/?q=https%3A%2F%2Fcasemedcare.org%2F&followRedirects=on>

<https://www.ssllabs.com/ssltest/analyze.html?d=ihk.img.co.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fihk.img.co.ug%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=ihk.img.co.ug>

<https://myip.ms/info/whois/50.22.208.143/k/748939688/website/ihk.img.co.ug>

<https://www.ssllabs.com/ssltest/analyze.html?d=nakaserohospital.com>

<https://securityheaders.com/?q=http%3A%2F%2Fnakaserohospital.com%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=nakaserohospital.com>

<https://myip.ms/info/whois/160.153.47.1/k/2375897079/website/nakaserohospital.com>

<https://www.ssllabs.com/ssltest/analyze.html?d=paragonhospital.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fparagonhospital.ug%2F&followRedirects=on>

<https://reports.exodus-privacy.eu.org/en/reports/149856/>

<https://www.ssllabs.com/ssltest/analyze.html?d=www.nssfug.org>

<https://securityheaders.com/?q=https%3A%2F%2Fwww.nssfug.org%2F&followRedirects=on>

<https://myip.ms/info/whois/104.40.3.53/k/1484673120/website/www.nssfug.org>

<https://www.ssllabs.com/ssltest/analyze.html?d=urbra.go.ug>

<https://securityheaders.com/?q=https%3A%2F%2Furbra.go.ug%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=urbra.go.ug>

<https://myip.ms/info/whois/154.72.194.115/k/1831083193/website/urbra.go.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fwww.mtn.co.ug%2F>

<https://myip.ms/info/whois/41.210.130.172/k/2237717804/website/www.mtn.co.ug>

<https://www.ssllabs.com/ssltest/analyze.html?d=www.mtn.co.ug>

<https://reports.exodus-privacy.eu.org/en/reports/154595/>

<https://reports.exodus-privacy.eu.org/en/analysis/258400/>

<https://www.ssllabs.com/ssltest/analyze.html?d=www.airtel.co.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fwww.airtel.co.ug%2F&followRedirects=on>

<https://themarkup.org/blacklight?url=www.airtel.co.ug>

<https://myip.ms/info/whois/41.223.58.200/k/3158352025/website/www.airtel.co.ug>

<https://play.google.com/store/apps/details?id=com.africell.africellapp>

<https://reports.exodus-privacy.eu.org/en/reports/149855/>

<https://www.ssllabs.com/ssltest/analyze.html?d=africell.ug>

<https://securityheaders.com/?q=https%3A%2F%2Fafricell.ug%2F&followRedirects=on>

<https://myip.ms/info/whois/197.157.8.15/k/848301909/website/africell.ug>

<https://www.ssllabs.com/ssltest/analyze.html?d=www.utl.co.ug>

<https://themarkup.org/blacklight?url=www.utl.co.ug>



