WHICH INTERMEDIARIES HAVE YOUR BACK?

How Kenyan Intermediaries Protect Human Rights Online

January 2019

KICTAnet
KENYA ICT ACTION NETWORK

TABLE OF CONTENTS:

01 : INTODUCTION

02: RESULTS AND ANALYSIS

03: FINDINGS – REVIEW OF COMPANY POLICIES ON PRIVACY

04: USER PERSPECTIVES ON INTERMEDIARIES

05: CONCLUSION AND RECOMMENDATIONS

Acknowledgement

The Kenya ICT Action Network is grateful to network members and the larger community from bloggers, application developers, start-ups, academia, journalists, artistes, civil society organisations and others who shared their experieces on privacy practices in the country.

We would also like to thank the team of researchers led by Riva Jalipa, assisted by Tracy Kadesa, Christine Waguma and Boniface Witaba. Riva Jalipa also wrote this report. Our gratitude also goes to the editorial team - Victor Kapiyo, Grace Githaiga and Grace Mutung'u.

Special mention to Renegade Ventures- the film crew who not only documented interviews with key experts but also shared their insights on contemporary privacy practices.

Many thanks to the administrative team- Mwara Gichanga and Anne Mwaura for facilitating the logistics of the project.

This work would not have been realised without the support of our partners. Shukran therefore to Association for Progressive Communications (APC) and the Swedish International Development Cooperation Agency.

Design and Layout: Amos Ochieng/MEDIAFORCE - mfc.ke

About KICTANet

KICTANet is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development.

Executive Summary

With greater internet penetration, Kenyans are increasingly using smartphones to access the internet. These gadgets ubiquitously track and generate personal data. They also facilitate numerous applications (apps) provided by third party developers. Some of the trends in app development include betting as well as mobile loan apps. These apps depend on analysis of personal data of the mobile user to offer their services. Such data is of interest to many other parties such as law enforcement, marketers and political actors. How then are users protected from their data being unjustly accessed by third parties?

This study sought to assess the extent to which local intermediaries in Kenya promote digital rights with the overall objective of advocacy for improved human rights based intermediary policies. The research is part of a year-long project to initiate discourse and make policy recommendations for internet intermediaries to clarify their rights and responsibilities. The project also aims to create and develop awareness and dialogue about digital rights in relation to intermediaries, thus promote informed usage of intermediary products. A bigger picture goal of this research is to contribute to knowledge on how technology affects the Kenyan society.

The study established that there are still challenges in how internet intermediaries handle the rights of consumers who utilize their services. This is exarberated by the increased of uptake of their services on one hand and absence of a clear legal and policy regime on the other. Without regulations detailing the rights of users and the duties of internet intermediaries, there is a likelihood that human rights of the users are possibly abused or violated. Lack of simple avenues for redress was also identified as a pitfall in achievement of digital rights through internet intermediaries.

In addition, the study observes that internet intermediaries have adopted varying policies and practices largely to foster their business interests rather than protect the rights of users. Moreover, the level of awareness among users on their human rights online remains wanting. Neither the users, nor the companies appear to recognise the importance of awareness. This therefore calls for urgent action by governments and all relevant stakeholders to work towards addressing this issues.

The research calls upon the internet intermediaries to revise their terms of use and privacy policies to make them digital rights based. In addition, be more open, produce annual transparency reports relating to how user data is handled, used and protected, and educate their users. Civil society actors are called upon to promote awareness for consumers on their digital rights, monitor the practices of intermediaries and highlight breaches whenever they occur. In addition, regulate the excesses and seal the gaps being exploited by intermediaries. In the same vein, academia is urged to conduct more research on best practices in respect to the various business models of intermediaries, including the extent to which companies practice the commitments in their policies. It is recommended that the government enacts robust legislation to secure the rights of users, and oversee the policies and practices of intermediaries.

1: INTRODUCTION

1.1 Background

The policies and practices of internet companies affect freedom of expression, among other rights online. Often the company policies are not available to users. Likewise, reports on their practices are not widely known or understood. Examples of these include how companies handle take-down requests, including the number, nature and the sources of the requests; how they respond to them; and whether they prepare transparency reports.

A majority of internet users in Kenya have little or no knowledge of the implications of using the services provided by internet intermediaries. Consequently, they grant power over their online transactions and communications for example, to intermediaries who in turn may abuse or violate their rights. In a context where there is an increasing uptake and development of local technology, as well as state interest to control the freedom of expression through intermediaries, the role of intermediaries to promote and protect human rights while also understanding their liabilities is significant.

This study forms part of a year-long project to initiate discourse and promote policy recommendations for intermediaries in terms of clarifying rights and responsibilities. The project also aims to create awareness about digital rights among the public as well as groups such as application developers. This is with the objective of promoting informed usage of intermediary products. In particular, this study aimed to assess the extent to which local intermediaries in Kenya promote digital rights with a means to improve the policies of intermediaries in terms of human rights online.

1.2 Country Context

Kenya hosts a population of 48.47 million people, 43.33 million of which are internet users meaning that internet penetration is at 89.4 percent.[1] There are 242 internet service providers with the largest shares of the market held by telecommunication companies such as Safaricom with 71.9 percent of the market, Airtel Networks Limited with 16.3 percent, and Finserve Africa Limited with 0.2 per cent.

Information and Communication Technologies (ICTs) have become crucial enablers of socio-economic development in Kenya. Besides being pivotal in sectors like telecommunications and financial intermediation, ICTs are increasingly being applied across all the economic activities most notably health, education and public administration.

There has been a continued decline of both international incoming and outgoing voice traffic which has been attributed to the growing uptake of Over-The-Top (OTT) applications such as Whatsapp and Facebook Messaging. The Communications Authority reported international incoming mobile traffic decreased from 742,481,905 minutes in the FY 2015/16 to 568,488,623 minutes in FY 2016/17.

Similarly, outgoing international traffic dropped marginally from 485,351,241 minutes registered in the previous period to 462,006,950 minutes registered in the period under review.[2] This shows the advancement of the local internet economy and illustrates the importance of internet intermediaries in promoting oe deterring digital freedoms. As shall be shown in the study, there are many global companies whose applications are used in the country. The policies and practices of global intermediaries, as well as trends in their regulation has an impact on the regulation of intermediaries in Kenya and in effect on the digital rights of end users.

1 Kenya - Internet Usage Stats and Market Reports https://www.internetworldstats.com/af/ke.htm accessed on December 29, 2018

2 Communications Authority, Annual Report for the Financial Year 2016-2017, p42, available at: https://ca.go.ke/wp-content/uploads/2018/04/Annual-Report-for-the-Financial-Year-2016-2017.pdf accessed on December 31, 2018

1.3 Literature Review

There are a number of studies that have reviewed the liability of intermediaries in Kenya. These comprise several research reports and presentations[3] which outline the regulatory environment,[4] the practices of intermediaries,[5] forms of censorship such as internet traffic tampering[6] and SMS blocking[7].

The studies call for the need to explore a variety of approaches when dealing with the issues of intermediary liability. These include legislation, co-regulation, self-regulation, tools and guidance for content management, development of new business models, collaboration with law enforcement and prompt responses to notices of illegal activity and content.

Some emerging issues and challenges noted in these studies include: indecision over which institutions should regulate internet intermediaries; inadequacy of consumer protection provisions; and the lack of robust privacy and data protection legislation. Other issues include the anti-competitive behaviour and monopolistic practices of intermediaries, the need for regulators to accommodate emerging technologies and to enhance their ability to regulate them. Moreover, there is still debate on the extent to which regulators should control or intervene in cases of copyright infringement, defamation, hate speech and terrorism on online platforms[8].

A majority of internet users in Kenya have little or no knowledge of the implications of using the services provided by internet intermediaries.

3 Centre for Internet and Society, Stanford Law School, 'WILMap: Kenya', Accessed: 13 September 2017, http://cyberlaw.stanford.edu/page/wilmap-kenya; Mpesa Regulatory Framework https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/wanjau_e.pdf accessed on 12 September, 2018

4 Alice Munyua, Grace Githaiga and Victor Kapiyo, 'Intermediary Liability in Kenya', Association for Progressive Communications, 2012, Accessed: 13 September 2017, http://www.apc.org/sites/default/files/Intermediary_Liability_in_Kenya.pdf; Mutemi, M., Walubengo, J., 'Treatment of Kenya's Internet Intermediaries under the Computer Misuse and Cybercrimes Act, 2018' available at: https://www.researchgate.net/publication/329160797_Treatment_of_Kenya's_Internet_Intermediaries_under_the_Computer_Misuse_and_Cybercrimes_Act_2018 accessed on December 31, 2018; State of Internet Freedom in Africa 2017: Intermediaries' Role in Advancing Internet Freedom – Challenges and Prospects, CIPESA https://www.opennetafrica.org/?wpfb_dl=74

5 Digital Rights in Sub-Saharan Africa, Analysis of Practices of Orange in Senegal and Safaricom in Kenya, Internet Without Borders https://www.accessnow.org/cms/assets/uploads/2018/02/RDR-Africa_Final-version-5_January-2018.pdf accessed on June 19, 2018

6 CIPIT, Strathmore University Law School, 'Safaricom and Internet Traffic Tampering', March 2017, Accessed: 13 September 2017, http://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf

7 Institute for Human Rights and Business, 'Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections', November 2013, Accessed: 13 September 2017, https://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf

8 Centre for Internet and Society, 'Intermediary Liability', http://cyberlaw.stanford.edu/focus-areas/intermediary-liability

1.4 Methodology

This study sought to understand the policy framework around intermediary liability in Kenya from the perspective of intermediaries as well as users. For intermediaries, researchers analysed the disclosed policies of a variety of internet companies categorised as telecommunication companies, e-commerce companies and service providers.

These included telecommunication providers, such as Safaricom, Airtel and Zuku; fintech mobile money and mobile loan providers, such as Mpesa, Airtel Money, and Tala; Sports betting companies such as Sportpesa and Betin; e-commerce platforms, such as Jumia and OLX; and taxi service providers such as Little Cab and Taxify, courier service providers such as Sendy; Kisafi, a cleaning services provider; Airbnb, an accommodation service provider, Truecaller, a caller identity application; and Tinder, a dating application. Though, most of the companies reviewed are considered "local", many are only local by name but are in fact based out of Kenya and sometimes subject to multiple jurisdictions. A few international intermediaries were therefore considered for comparative purposes.

The policies of each of the intermediaries were assessed on the basis and the extent to which they provided information relating to how they managed personal user data. Researchers considered whether they respected consumer rights including allowing users to access, correct and remove their data, and the available forms of redress for grievances. It should be noted that where one company provided more than one service, the company's' policies were assessed separately i.e. as different companies. For example, the policies of Safaricom (the telcom) were assessed separately from its mPesa service policies or Little Cab, a taxi service provider which Safaricom co-owns.

Where privacy policies were not available, "Terms and Conditions" or "Terms of Use" policies were analysed. Where these were not available, these were requested by email and by phone. Interviews were conducted among several intermediaries to seek information or clarification where it was lacking or unclear. There are a few intermediaries who did not respond or partially responded to our requests for information. For instance, one intermediary, Kisafi, declined to reveal their business location.

Results were then collated and analysed. The companies were subsequently ranked in the order of which company policies provided for the most detail, and were the most compliant with international data privacy principles and digital rights in general.

'Though most of the companies reviewed are considered "local", many are only local by name but are in fact based out of Kenya and sometimes subject to multiple jurisdictions'


I agree

2: RESULTS AND ANALYSIS

2.0 Framework for digital rights

Digital rights may be described as the rights to access to and control of digital information or the human rights which allow for the access, use, creation, and publishing of digital media or the access and use computers, other electronic devices, or communications network. They comprise the freedoms of expression, information, media, association and privacy.

2.1 International Instruments

There are several frameworks at the international level that support digital rights. The key instrument is the International Bill of Human Rights consisting of the Universal Declaration of Human Rights (UDHR, 1948), the International Covenant on Civil and Political Rights (ICCPR, 1966) with its two Optional Protocols and the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966)[9].

The African Charter on Human and People's Rights (ACHPR) also provides for these rights. Although ACHPR does not explicitly provide for privacy, African norm setting fora generally hold that article 5 of the charter which provides that every person has inherent dignity also includes the right to privacy[10]. Digital rights may also be extrapolated from declarations such as Declaration of the Principles of Freedom of Expression in Africa[11] . The African Charter on the Rights and Welfare of the Child, also guarantees protection of privacy for children in article 10[12] .

In addition, the United Nations Guiding Principles on Business and Human Rights is a useful tool for ensuring the protection of human rights from a business perspective. The instrument comprises 31 principles that guide the implementation of the United Nations 'Protect, Respect and Remedy' framework on human rights and transnational corporations, and other business enterprises[13].

2.2 Other Regional Instruments

The General Data Protection Regulation (GDPR) is a regulation in the European Union that provides the legal framework for data protection and privacy for all individuals within the European Union (EU), the European Economic Area (EEA), and beyond. It addresses the export of personal data outside the EU and EEA areas. It came into effect on May 28, 2018 having been developed in April, 2016[14].

The GDPR enumerates several principles for data protection, which include: breach notifications; the right of access by data subjects to their data; the right to be forgotten; data portability; privacy by design; and certain requirements for data protection officers. Whereas Kenya is not a member of the EU, the GDPR provides a useful benchmark for safeguarding personal data.

2.3 The Constitution of Kenya, 2010

The Constitution of Kenya guarantees the right to privacy (Article 31), freedom of expression (Article 33), freedom of the media (Article 34), access to information (Article 35), freedom of association (Article 36) and consumer protection rights (Article 46) in its Bill of Rights. All of these apply to human rights online or digital rights.

9 International Bill of Human Rights https://www.ohchr.org/documents/publications/compilation1.1en.pdf

10 African Charter on Human and People's Rights http://www.achpr.org/instruments/achpr/

11 Declaration on Freedom of Expression Principles in Africa (2002) http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html

12 The African Charter on the Rights and Welfare of the Child (ACRWC) https://au.int/en/documents-45

13 Guiding Principles on Business and Human Rights:

Implementing the United Nations 'Protect, Respect and Remedy' Framework https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

14 The EU General Data Protection Regulation (GDPR) https://eugdpr.org/

2.4 Kenya Information and Communications Act (KICA)

KICA is Kenya's basic ICT law and it contains several provisions relating to intermediary liability. For example, section 27 of the Act empowers the Cabinet Secretary in charge of communications to make rules in consultation with the Communications Authority pertaining to the telecommunications system. This means that the Cabinet Secretary may introduce new obligations for intermediaries.

Section 30 of the Act prohibits the intentional modification or interference with the contents of a message sent by means of a telecommunication system, by persons licensed to run a telecommunication system. Section 31 prohibits licensed operators from intercepting or disclosing the contents of a message sent through the system while section 46(I) of the Act lists the responsibilities of broadcasters to include the respect of the rights to privacy of individuals and the copyrights or any neighbouring right to any work or material. Section 84(D) of the Act further prohibits the publishing or transmission of obscene information in electronic form. Section 93 of the Act provides general restrictions on disclosure of information.

2.5 Computer Misuse and Cybercrimes Act, 2018

The Computer Misuse and Cybercrimes Act is a recent legislation that provides for among others: offences relating to computer systems; enabling the timely and effective collection of forensic material for use as evidence; and the facilitation of international cooperation in the fight against cybercrime. It provides for cybercrimes such as unauthorised access, access with intent to commit a further offence, unauthorised interference, unauthorised interception, provision and use of illegal devices and access codes, and unauthorised disclosure of passwords.[15] It also provides for content related offences [16] including child pornography[17]. Section 27 of the Act prohibits cyberstalking and cyberbullying. Part IV of the Act provides for investigation procedures to be undertaken when obtaining evidentiary material in computer systems, subscriber information, traffic data and content data. Sections of the Act are currently suspended pending determination of a petition against their provisions.

2.6 Data Protection Bills

Currently, there is a data protection bill by the Senate ICT Committee and a draft bill under the auspices of a taskforce under the Ministry of ICT. Both proposals aim to give effect to Article 31(c) and (d) of the Constitution on the right to privacy. They also seek to among others: establish an office of a data protection commissioner; regulate the processing of personal data; provide for the rights of data subjects and, for the obligations of data controllers and processors.

The study was two pronged: first, policies of intermediaries were reviewed, after which a user perception survey was carried out. This section describes the findings.

15 Sections 15 - 19 respectively of the Computer Misuse and Cybercrimes Act

16 Section 22 makes it a crime to publish false information with the intent that the information be acted on as authentic

17 Section 24 prohibits the delivery, transmission, or distribution of child pornography, making the same available in any way and the possession of child pornographic material in a computer system or computer data storage medium.

3: FINDINGS - REVIEW OF COMPANY POLICIES ON PRIVACY

3.1 Sample of Intermediaries

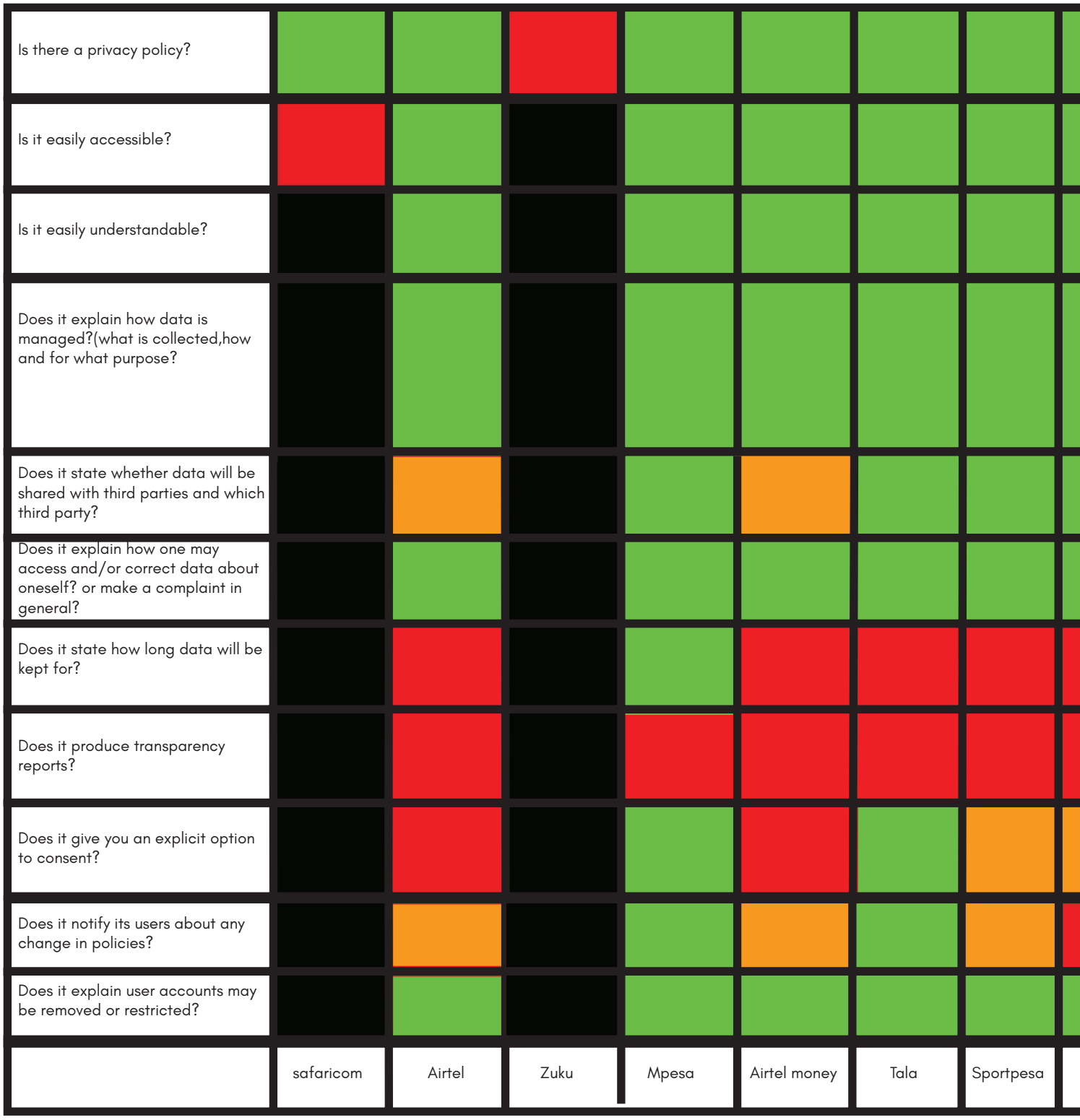
The study as part of its review of the policies of intermediaries in Kenya undertook to frame the key digital rights issues as found in the GDPR in the form of binary (yes or no) questions. Each intermediary's policies such as their privacy policy or terms of use were then reviewed in line with the formulated questions. As shown in the table below, positive responses were highlighted in green, partial answers in orange and negative answers in red. Arears marked in black denoted null or not applicable, especially where the previous questions were in the negative.

Several companies comprising telcos, fintech providers, and e-commerce platforms were assesed. The analysed companies provide services such transport and deliveries, accommodation, cleaning, loans, online shopping and caller details were analysed. They were selected on the basis of the services they provided in the Kenyan market or popularity in the the East Africa region.

Intermediary service	Description
Airbnb	A global hospitality site
Airtel	A local mobile network operator
Airtel Money	A local mobile money service
Betin	A local mobile/online betting service
Jumia	A locally available e-commerce service
Kisafi	A local house cleaning service app
Littlecab	A locally available cab hailing app
Mpesa	A Kenyan based mobile money service
OLX	A locally available e-commerce service
Safaricom	A local mobile network operator
Sendy	A locally available *bodaboda* (motobike) hailing/delivery service
Sportpesa	A local mobile/online betting service
Tala	A locally available mobile loan app
Taxify	A locally available cab hailing app
Tinder	A global dating site
Truecaller	A global phone number app
Zuku	A local ISP providing home fibre

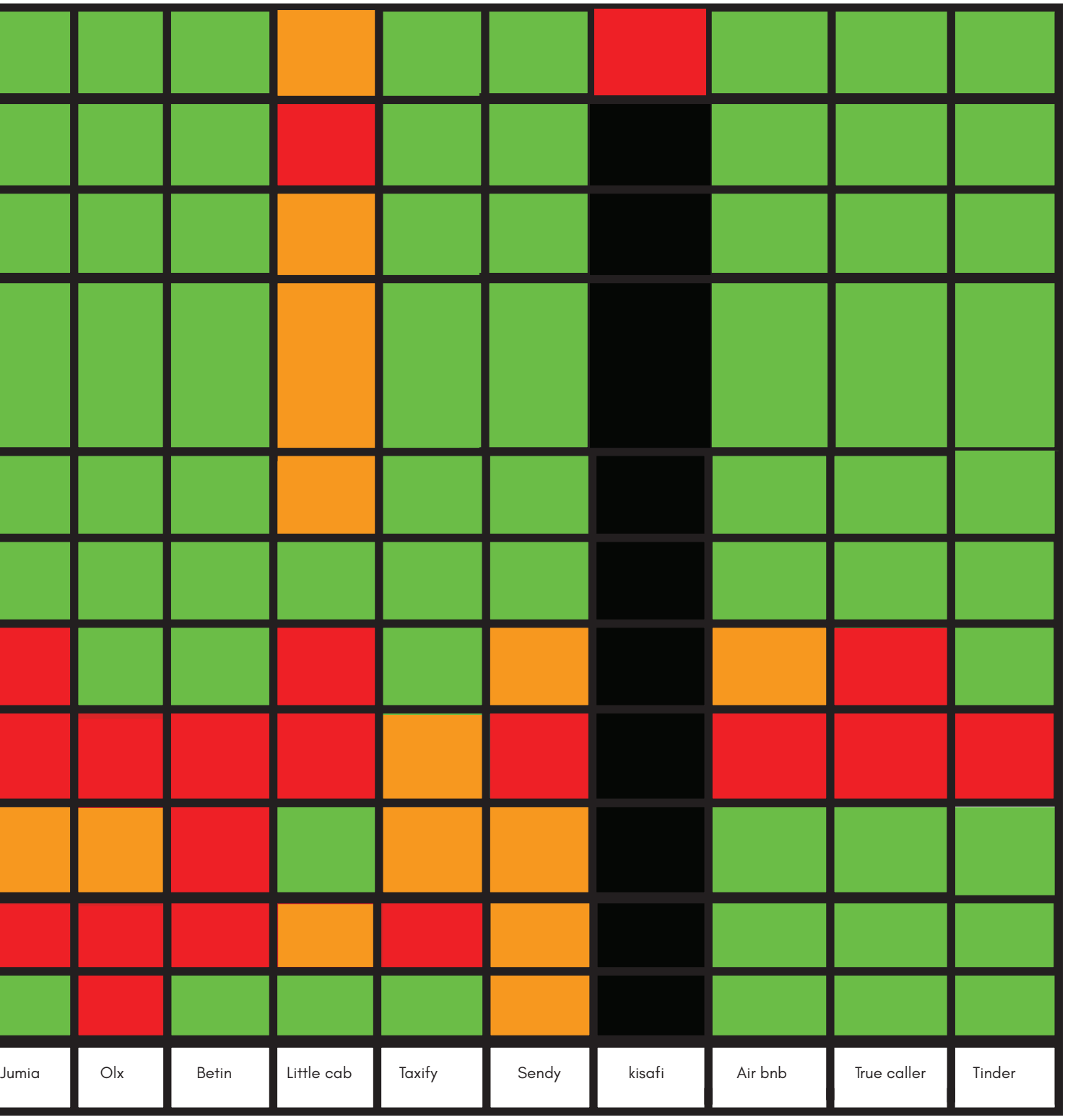
Table 1: Description of intermediaries reviewed

The intermediaries were then ranked based on the availability, accessibility, simplicity as well as how they disclosed information about their data sharing, correction and retention policies. They were also assesed for providing information on transparency reports, facilitating informed consent and user notifications.



	Yes
	Partial
	No
	Null or not applicable

Table 2: Review of the Disclosed Policies of Intermediaries in Kenya


Jumia
Olx
Betin
Little cab
Taxify
Sendy
kisafi
Air bnb
True caller
Tinder

Most of the companies were found to have stand alone privacy policies or a privacy clause in their terms and conditions found on their respective websites. The exceptions were Safaricom, Zuku and Kisafi. Little Cab terms and conditions were noted to contain a few provisions on privacy and further indicated that there was a privacy policy. The policy was however, not available on the website or on their mobile application. A number of companies' made their privacy policies easily accessible and were available on the homepages of their official websites. In terms of ease of understanding, most were easy to read and they were not full of legal and technical language except for Little Cab[18].

3.2 Localisation of global companies

Certain intermediaries appeared to be "local" intermediaries because of their Swahili names. However, on further examination of their terms and conditions and privacy policies, they were found to be registered outside of Kenya. For example, Tala, formerly Mkopo Rahisi (meaning "easily in hand") is registered in California. Sportpesa (meaning "Sportmoney"), while registered in Kenya, is a subsidiary of a company registered in the UK. Jumia (similar in sound to "Jumuia" meaning "community") is registered in Germany. Sendy discloses that its data will be transferred, processed and stored in the Republic of Ireland meaning that it is also registered in Ireland. Further, Truecaller provides for contacts in India while Taxify is registered in Estonia.

This has both merits and demerits. On the one hand, the companies keep a lean staff that may not adequately respond to user issues in a localised manner. It is presumed that users benefit where there is strong data protection regulation in the country of registration of the company or where the data resides. This may explain the robustness policies such as those of Taxify (Estonia). Globalisation and localisation dictates the standards for data protection and privacy in terms of where data is processed and stored, and therefore governed.

It is worth noting that the Airtel policy was specific to the use of the website and not in relation to the use of Airtel for voice, SMS and data services. The company's website policy was found to be similar to the Airtel money policy. The study also noted that the mPesa policy needed to be more explicit on how data was collected technically.

3.3 Data Handling Practices

In the policies, some of the companies explained who they were as data handlers; what they did with users' data; what exactly they collected; how they collected the data; and how it was used. The international intermediaries were found to be more specific and descriptive in general as compared to the local intermediaries. In addition, the policies of international intermediaries were found to be generally simpler to read

3.3.1 Data Sharing

The GDPR also recommends companies to mention whether they share data, and with whom. Almost all the companies reviewed stated that they did share their data with third parties. However, where they were silent and did not provide information or explain who the third parties were.

Taxify, registered in Estonia, was the only intermediary in the sample where privacy policies could be viewed in different languages. There were also separate privacy policies for drivers and for users, available in different languages. In addition, it provided a link for Taxify group companies and partners to access personal data to the extent necessary to provide customer support in the respective country[19].

This framework by Taxify, appears to satisfy the GDPR requirement for collecting, processing and keeping data for legitimate interests. However, a more descriptive the policy is better as it allows the users to understand how their data is being handled hence they can make informed decisions.

3.3.2 Data Transfer

Most of the local companies made no mention of whether data in their custody could be transferred outside of their jurisdiction. The policies with data transfer information were wordy and in legal language. Sendy described how

18 Little Cab, Terms and Conditions. Available at: https://www.little.bz/ke/tnc.php accessed on January 2, 2019
19 Taxified Cities. https://taxify.eu/cities/

information would be transferred to the Republic of Ireland.[20] Airbnb on the other hand, is explicit about who processes a user's data, which is dependent on where one resides.[21] The company for example, refers to itself the "Data Controller", which if the country of residence of a user is the United States, Airbnb, Inc.; if outside of the United States, the People's Republic of China which does not include Hong Kong, Macau and Taiwan ("China") and Japan, Airbnb Ireland UC ("Airbnb Ireland"); if the residence is China, Airbnb Internet (Beijing) Co. Ltd ("Airbnb China"), and if the residence is Japan, Airbnb Global Services Limited ("Airbnb GSL"), and so on.

3.3.3 Data Correction

Most of the companies provided information on how a user could correct, update information or access their information. Airbnb and Truecaller, which collect and verify personal information require users to make correction requests. For example, Truecaller has explicit provisions to address grievances and update or correct data. Again, the international companies, in general, have more comprehensive, easier to read policies including on how a user can access information.

OLX has a similar provision for user requests:

Access, Correction and Deletion: For users that have created an account or listing with us, you can access, correct or delete your personal information by writing to us via our Contact Form. You are responsible for keeping the data you provide or post on our network accurate. If your account was created through an identity provider (e.g. Facebook Connect) you may also disable or change the account information through the settings offered by the identity provider (e.g. on Facebook.com).

3.3.4 Data Mininisation

OLX gives fair warning about how to limit giving data to it as well as limiting data processing by it.[22] The OLX privacy policy provides as below:

Third Party Choice: Certain third parties active on our site, e.g. Google Adwords, give you the ability to opt out of their collection and use of information for interest-based advertising. You can visit http://www.youronlinechoices.com or http://www.networkadvertising.org to learn more about this practice and to exercise choices over how this type of information may be collected and used.

Sendy takes the approach of giving the user the choice to minimise data[23] . Their policy provides:

- Targeted advertising (also known as Behavioral Advertising) uses information collected on an individual's web or mobile browsing behavior such as the pages they have visited or the searches they have made. This information is then used to select which advertisements should be displayed to a particular individual on websites other than our web site(s). For example, if you have shown a preference for nursing while visiting our website(s), you may be served an advertisement for nursing-related programs when you visit a site other than our web site(s). The information collected is only linked to an anonymous cookie ID (alphanumeric number); it does not include any information that could be linked back to a particular person, such as their name, address or credit card number. The information used for targeted advertising either comes from us or through third party website publishers.
- If you would like to opt out of targeted advertising from us that occurs when visiting our third party advertising publishers, please contact us at support@sendy.co.ke Please note that this will opt you out of targeted ads from our Company and any other participating advertisers. If you opt out, you may continue to receive online advertising from us; however, these ads may not be as relevant to you.
- In order for behavioral advertising opt-outs to work on your Device, your browser must be set to accept cookies. If you

20 Sendy's Privacy Policy provides for: Consent to Transfer Information to the Republic of Ireland

Please be aware that information we collect, including, Personal Information, will be transferred to, processed and stored in the Republic of Ireland . The data protection laws in the Republic of Ireland may differ from those of the country in which you are located, and your Personal Information may be subject to access requests from governments, courts, or law enforcement in the Republic of Ireland according to their laws. By using the Services or providing us with any information, you consent to this transfer, processing and storage of your information in the Republic of Ireland available at: https://sendyit.com/privacy accessed on January 2, 2019.

21 Privacy Policy, Airbnb, available at: https://www.airbnb.co.uk/terms/privacy_policy accessed on January 2, 2019

22 Privacy Policy, OLX available at: https://help.olx.co.ke/hc/en-us/articles/360000549865-Privacy-Policy accessed on January 2, 2019.

23 Data Privacy Policy, Sendy, available at: https://sendyit.com/privacy accessed on January 2, 2019.

delete cookies, buy a new Device, access our Services from a different device, login under a different screen name, or change web browsers, you will need to opt-out again. If your browser has scripting disabled, you do not need to opt out, as online behavioral advertising technology does not work when scripting is disabled. Please check your browser's security settings to validate whether scripting is active or disabled.

- Additionally, many network advertising programs allow you to view and manage the interest categories they have compiled from your online browsing activities. These interest categories help determine the types of targeted advertisements you may receive.

Sendy may close or suspend an account without prior warning for any contravention of its Terms and Conditions. Jumia prohibits the use of false email addresses.

3.3.5 Data Retention

A number of the intermediaries did not state the period within which data shall be retained. They also did not specify the criteria used to determine the duration the data can be kept.

Communications and fintech companies addressed the issue of retention by stating that they retained data for as long as a user had an account with them or as is required by law. For example, Betin and mPesa policies specifies that data will be retained for seven years or as required by law. OLX states that it will retain data "for as long as is required to fulfil the above business objectives".[24] Tinder stipulates that it will retain data for five years.

Taxify was the only intermediary in the study that specified the duration for different kinds of data:[25]

- Your personal data will be stored as long as you have an active passenger account. If your account is closed, personal data will be deleted (according to the policies set out in this section) from the databases, unless such data is required to be retained for accounting, dispute resolution or fraud prevention purposes.
- Financial data regarding transportation services provided to passengers will be stored for 3 years after the last journey.
- Data required for accounting purposes will be stored for 7 years [after the last journey].
- In the event that there are suspicions of a criminal offence, fraud or false information having been provided, the data will be stored for 10 years.
- In case of payment disputes, data will be retained until the claim is satisfied or the expiry date of such claims.
- Journey history data will be stored for 3 years, after which the data will be anonymized.
- Please note that the deinstallation of Taxify app in your device does not cause the deletion of your personal data.
- If the Taxify app has not been used for 3 years, we will notify you and ask you to confirm whether account is still active. If no reply is received, the account will be closed and personal data will be deleted unless such data is required to be stored for accounting, dispute resolution or fraud prevention purposes.

3.4 Informed consent

Most of the intermediaries stated that usage of their services meant consent to their terms and conditions, including privacy provisions effective upon signing in or using their services. Whereas they did not provide for an express consent option to the terms and conditions, the continued use of the applications was deemed to mean consent. In relation to Taxify, the company noted that if 'substantial amendments are made to the General Terms and Conditions" notification would be made to the user by email or through the Taxify app notifications.[26]

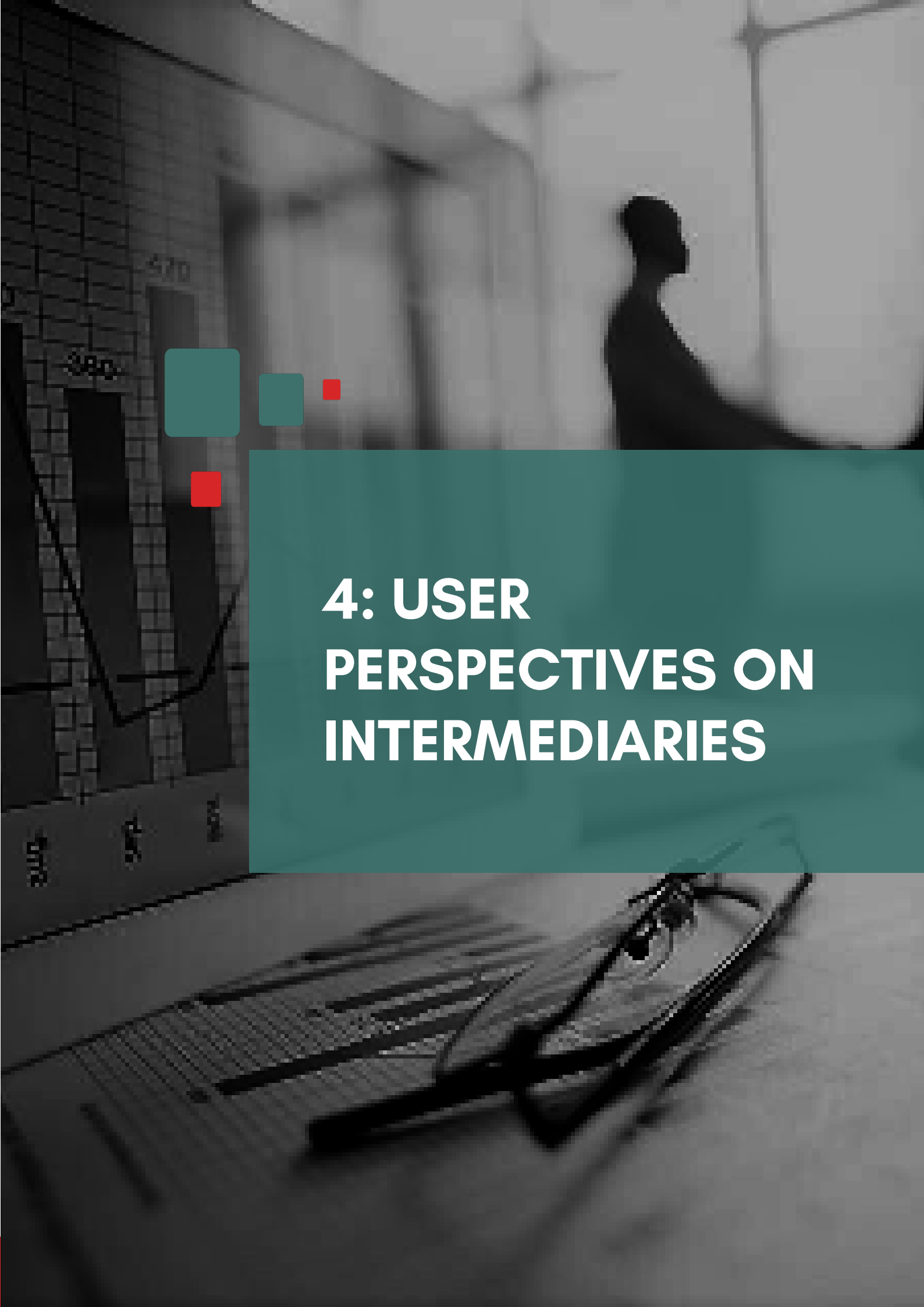
3.5 Transparency Reports

None of the intermediaries reviewed published transparency reports on the information requested from them of their users by different parties. Some, for example Safaricom mention that they may share information with third parties where required for legal reasons.

24 Privacy Policy, OLX available at: https://help.olx.co.ke/hc/en-us/articles/360000549865-Privacy-Policy accessed on January 2, 2019.
25 Privacy Notice for Drivers, Taxify, available at: https://taxify.eu/legal/privacy-for-drivers/#ke accessed on January 2, 2019
26 General Terms for Drivers, Taxify, available at: https://taxify.eu/legal/terms-for-drivers/ accessed on January 2, 2019

Taxify, registered in Estonia, was the only intermediary in the sample where privacy policies could be viewed in different languages.

Image: ZDNet.com



4: USER PERSPECTIVES ON INTERMEDIARIES

4.1 User samples

User perspectives were also reviewed to assess how they relate to the intermediaries. A total of 73 respondents from Kenya participated in the online survey. More than half of the respondents (53.42%) were within the age group of 18-24 years. A third of them (31.51%) were within the age group 25-34 years, while 13.7% were aged between 35-44 years. There were no respondents in the 45-54 years age group, although one respondent was above 55 years old.

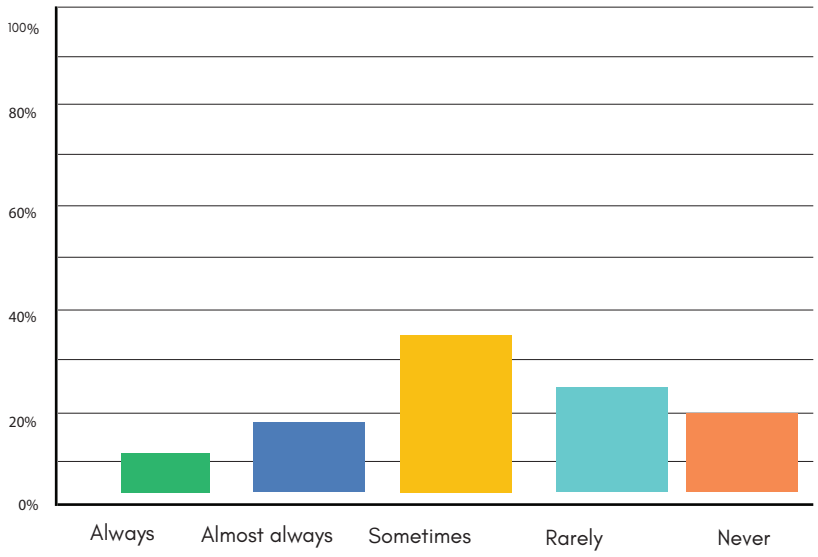
There was near gender parity among the respondents with 52.05% identifying as male and 47.95% as female. Most had achieved post high-school level education with only 5.48% reaching high school level. 8.22% indicated receiving vocational/technical training post high-school, 69.86% indicated achieving degree level education, 10.96% indicated to have achieved masters degrees while one respondent indicated having achieved a doctoral degree. The questions were tailored to evaluate how ordinary internet users understood the privacy policies of intermediaries before using their services.

In addition to the survey, a focus group discussion among artistes was carried out. Validation of the research findings also provided input from users on privacy practices.

4.2 Reading Privacy Policies

The respondents were asked how often do they read the terms of use or privacy policies before making use of an application or online service. As shown in the table below, almost a third of respondents, or 36.99% indicated that they read the terms of use of privacy policies "sometimes" before using an application or online service.

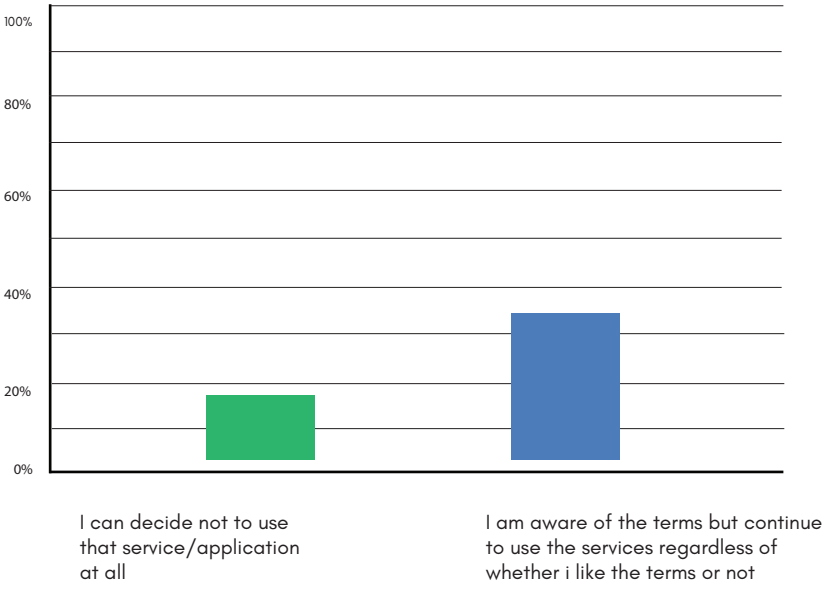
In addition, 24.66% of the respondents reported that they "rarely" read the terms while 16.44% reported "never" reading the terms.



Further, 12.33% reported "almost always" and 9.59% reported "always" reading the terms. Most users therefore rarely read the policies indicating a lack of interest by users in being aware of what policies intermediaries provide.

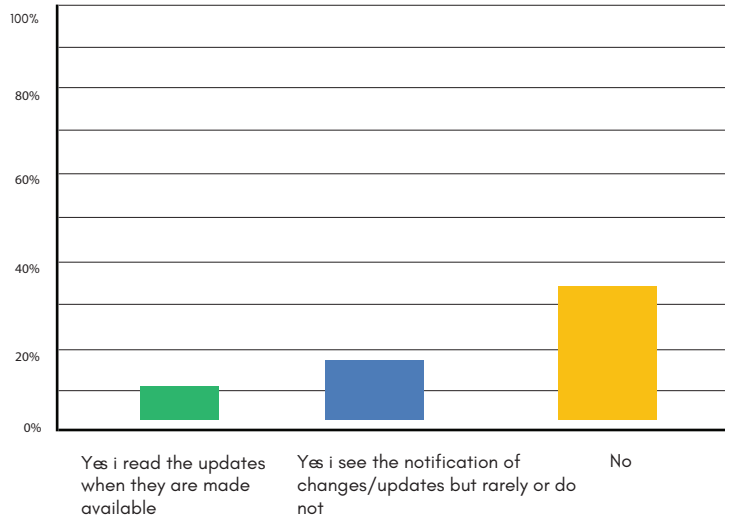
4.3 How Policies Affect Users

The study sought to establish the effect of policies on the respondents. As shown in the table below, for those who indicated that they read the policies, 55.56% opted to continue using the service whether or not they agreed with or liked them. This indicated an apathy for their own digital rights. Further, 44.44% of the respondents reported choosing not to use the service or application, indicating a significant level of awareness on their rights.



4.4 Awareness on Changes to Policies

As shown in the table below, 46.58% of the respondents indicated that they were aware of the changes or updates to the terms of conditions or privacy policies. However, they did not thoroughly read and understand them. User apathy may be inferred.



Further, 31.51% of the respondents reported not being aware of the changes or updates. 21.92% of the respondents reported taking an active interest in reading the updates when they were made available. This indicates that there exists a significant proportion of users who take an active interest in knowing about and acting on their digital rights.

5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

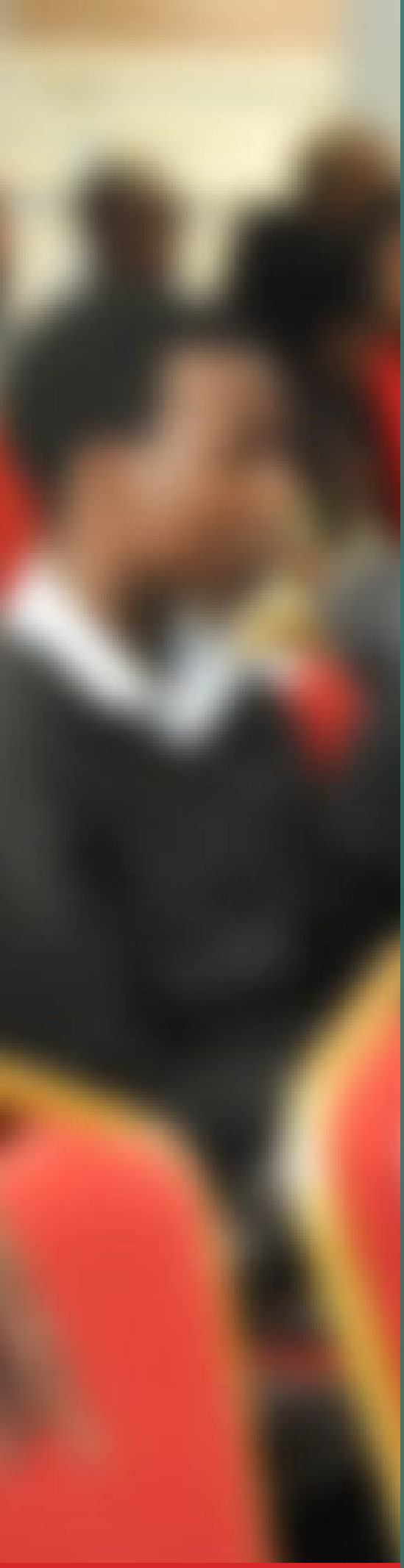
It has emerged from the study that most companies did not have privacy policies until the GDPR came into effect in May, 2018. Those that did, updated them shortly before or after May, 2018. Those who continue not to have privacy policies such as Kisafi did not fully respond to email requests about the same, despite the Access to Information Act (ATI) being in force since September 2016.

It could be inferred from the study sample that the bigger the intermediary, the more robust the policies and accountability. This underscores the need for awareness and assistance to micro, small and medium enterprises (MSMEs) to upgrade their policies so that they uphold digital rights.

Mobile money privacy policies were found to be more explicit or comprehensive as compared to the voice and internet policies.The research was however unable to assess the extent to which the intermediaries implement commitments in their policies, for example, data minimisation and data retention. This is an area for future research.

The findings indicate the urgency for sensitisation of users of their privacy online. Even where intermediaries make information available, users do not always read them and they are therefore not adequately informed and empowered to pursue their rights online.

It has emerged from the study that most companies did not have privacy policies until the GDPR came into effect in May, 2018



5.2 Recommendations

5.2.1 Intermediaries

- Intermediaries need to upgrade their privacy policies to uphold digital rights including freedom of expression, access to information and the right to privacy.
- Intermediaries should produce annual transparency reports relating to how user data is handled.
- Intermediaries should disclose how long they hold information, how they use the information they hold, and how they safeguard and protect it.
- Intermediaries should educate their users on their rights when using their services.

5.2.2 Civil Society Organisations (CSOs)

- Civil society organizations should promote more awareness for consumers on privacy online and other digital rights.
- Civil society organizations should monitor the practices of intermediaries and highlight breaches whenever they occur.
- Noting that Kenya has multiple avenues for public engagement, CSOs should advocate for rights based regulation
- Engage policy makers to have responsive policies for MSMEs

5.2.3 Government

- The government should adopt robust legislation to secure the rights of users, oversee the policies and practices of intermediaries and regulate the excesses and seal the gaps being exploited by intermediaries.
- Lead by example by implementing the highest standards of privacy where its organs or departments are intermediaries

5.2.4 Academia

- Academia should research on best practices with respect to the various business models of intermediaries, including the extent to which companies actually practice the commitments in their policies.
- Prepare future generations for the practice of privacy through education on issues such as privacy by design
- Provide thought leadership in designing a rights-based information economy that best serves a middle income country like Kenya

Prepare future generations for the practice of privacy through education on issues such as privacy by design

BIBLIOGRAPHY

1. Company Privacy Policies
2. Airbnb Privacy Policy: https://www.airbnb.co.uk/terms/privacy_policy last updated November 9, 2018
3. Little Cab Terms and Conditions: https://www.little.bz/ke/tnc.php
4. Mpesa Privacy Policy: http://safaricomapp.safaricom.co.ke/mc/resources/privacypolicy.htm
5. Mpesa Terms and Conditions: https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/M-PESA_CUSTOMER_TERMS_AND_CONDITIONS.pdf
6. OLX Privacy Policy: https://help.olx.co.ke/hc/en-us/articles/360000549865-Privacy-Policy last updated February, 2016
7. Sendy Data Privacy Policy: https://sendyit.com/privacy last updated June 22, 2018
8. Taxify Privacy Notice for Drivers (in Kenya): https://taxify.eu/legal/privacy-for-drivers/#ke
9. Airtel Kenya terms and conditions https://www.airtelkenya.com/termCondition
10. Jumia Kenya privacy policy https://www.jumia.co.ke/privacy/
11. Betin privacy policy https://web.betin.co.ke/pages/SportFooter_Privacy/guest
12. Zuku terms and conditions http://www.zuku.co.ke/terms-and-conditions/
13. Sportpesa terms and conditions https://www.sportpesa.co.ke/terms_and_conditions

ANNEX

User Survey Questions: Users' Awareness of online Privacy Policy

Demography
Age:
- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55+

Gender:
- Male
- Female

Education:
- High school graduate
- Technical/vocational training
- Bachelor's degree
- Master's degree
- Doctorate degree

County:
1. How often do you read the terms of use or privacy policies before making use of an application/ online service?
    a. Always
    b. Almost always
    c. Sometimes
    d. Rarely
    e. Never

2. If you do read these policies, to what extent do they affect you?
a. I can decide not to use that service/application at all
b. I am aware of the terms but continue to use the service regardless of whether I like the terms or not

3. Are you ever aware of changes and or updates to the terms and conditions or privacy policies?
a. Yes I read the updates when they are made available
b. Yes I see the notification of changes/updates but rarely or do not check on what has changed
c. No

4. Are you aware of methods that can be used to collect usage information, e.g cookies, web beacons, adds and how to prevent them from accessing your information?
a. Yes
b. No
5. Are there any experiences you would like to share?

KaribuKICTANet :
We invite you to partner

KICTANet
KENYA ICT ACTION NETWORK

Follow us on twitter @KICTANet
www.kictanet.or.ke
Email: info@kictanet.or.ke