PRIVACY & DATA PROTECTION PRACTICES OF DIGITAL LENDING APPS IN KENYA



Strathmore University

Centre for Intellectual Property and Information Technology Law

TABLE OF CONTENTS

Privacy And Data Protection Practices Of Digital Lending Apps In Kenya 3

1. Introduction 3

2. Literature Review 5

3. The DPA And Digital Lending Apps 8

3.1 Data Protection Principles 8

3.2 Other relevant provisions of the DPA 9

3.2.1 Rights of the data subject 9

3.2.2 Collection of data from the data subject 9

3.2.3 Notification and information 9

3.2.4 DPIA 9

3.2.5 Protection from automated decision-making 10

3.3.6 Data portability 10

3.3.7 Data protection by design and default 10

4. The Study 11

4.1 Methodology 11

4.1.1 Apps selection 11

4.1.2 App permissions 12

4.1.3 Trackers 12

4.2 Challenges And Limitations 12

4.2.1 Legality of traffic monitoring 12

4.2.2 Unavailability of appropriate phones for the study locally 13

5. Data Collection 14

5.1 App permissions 14

5.1.1 Discussion 17

5.2 Digital lending apps and third-party data-sharing 17

5.2.1 Discussion 21

5.3 Checking data on trackers 22

5.3.1 Discussion 26

5.4 Summary of findings 27

6. Conclusion 29

Strathmore University

Centre for Intellectual Property and Information Technology Law

PRIVACY AND DATA PROTECTION PRACTICES OF DIGITAL LENDING APPS IN KENYA

1. INTRODUCTION

The Centre for Intellectual Property and Information Technology Law (CIPIT) has been studying the impact of digital identities on society.[1] This has included policy research on the legal and technical aspects of the national digital ID system Huduma Namba under which the Government is integrating all its identification documents. Our research shows that the national digital identity system also integrates with privately issued digital identities such as mobile phone numbers and social media accounts.[2] We anticipate that as national digital ID uses increase, so will the linkage with private systems. This is already evident from e-government services, where payments for Government services, such as passport applications, drivers' licences, national health insurance and hospital bills in public hospitals are made using mobile money platforms. We also appreciate that private digital ID is more developed and has more uses than national digital ID. For example, a 2019 survey, undertaken by the Central Bank of Kenya (CBK), estimates that access to financial products had risen from 26.7% in 2006 to 89% of the population in 2019. This is attributed partly to the availability of digital products such as 'mobile banking, agency banking, digital finance and mobile apps'.[3] These products make use of personal data, which broadly falls under digital identities. This study seeks to understand the privacy implications of digital ID by looking at digital lending apps.

Digital lending is a relatively new phenomenon in Kenya. It builds upon existing systems such as microfinance as well as mobile money. Microfinance may be defined as financial mechanisms targeting low-income individuals who lack access to traditional banking services.[4] Unlike conventional banking that requires collateral in the form of property, microfinance uses non-property guarantees for loans such as social reputation, financing to women's groups as opposed to individuals, and other innovative guarantees. Building on this, digital lending leverages on behavioural data collected as one uses a mobile phone. Examples of such data include type of phone, location, contacts, apps and mobile money transactions.

1 CIPIT, 'Digital ID' < https://cipit.strathmore.edu/digital-id/> on 4 November 2020.

2 Caribou Digital, 'Kenya's Identity Ecosystem', Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2019< https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf> on 4 November 2020.

3 FSD and Central Bank of Kenya, 'FinAccess Household Survey' 2019, p.8. <https://www.centralbank.go.ke/uploads/financial_inclusion/2050404730_FinAccess%202019%20Household%20Survey-%20Jun.%2014%20Version.pdf> 25 Jan 2021

4 Section 2 and 3 Microfinance Act, 2006.

The 2019 FinAccess household survey estimates that about 14% of Kenyan adults have taken a digital loan, either through mobile banking or an app.[5] Literature traces the history of mobile lending in Kenya to the growth of mobile money services such as Mpesa.[6] From 2012, Safaricom, which operates Mpesa, began offering mobile loans known as Mshwari. Banks also joined in and began offering digital loans through products such as KCB-Mpesa by KCB Bank and Eazzy Loan by Equity Bank. They have been joined by financial technology (fintech) apps like Branch, Tala and Okash more recently. These apps, which require one to have a smartphone, rely on behavioural data to determine creditworthiness. This study is concerned with the privacy practices of digital lending apps. It begins with a brief literature review on digital lending apps, finding that previous studies, particularly local ones, have focussed on non-data aspects of the apps. Global policy-making bodies have mooted personal data or digital ID as a means to financial inclusion; thus, this study analyses how the primary law on personal data in Kenya, the Data Protection Act (DPA), applies to digital lending apps. It goes further to test how privacy and data protection are applied by considering the permissions that several of the popular apps require, as well as the servers that the apps connect to.

5 FSD and CBK, 'FinAccess Survey'.p.5.

6 Keith B, 'The Failure of the 'single Source of Truth' about Kenyans: The NDRS, Collateral Mysteries and the Safaricom Monopoly' 78, *Journal of African Studies*, 2019, 91.

2. LITERATURE REVIEW

A preponderant amount of the literature reviewed approaches digital lending from development perspectives, focusing on its potential for poverty reduction and financial inclusion. There is also literature considering the data aspects of financial inclusion, thereby linking digital ID and fintech.

Issues from a development perspective include the impact of mobile loans on overall income and wealth,[7] household access to digital loans,[8] loan pricing[9] and financial literacy.[10] Research around financial inclusion has also included studies[11] and experiments[12] with financial products targeting low-income earners. There is also critique on the financial inclusion rationale in digital lending, with some studies highlighting the inequality created between borrowers and the app owners.[13] For example, the borrowers – who are often poor – are indebted, sometimes perpetually, as they borrow small sums to meet basic needs while keeping their credit profile positive.

The role of digital technologies such as fintech in alleviating the effect of the COVID-19 pandemic cannot be gainsaid.[14] Locally, the CBK suspended transaction charges on person-to-person mobile money transfers of up to 1000 Kenya Shillings, so as to encourage cashless transactions. [15] A similar directive was given for bank account to mobile money transfers. The directives were extended until the end of 2020. In April 2020, CBK also locked out digital lenders from credit information sharing services by barring them from submitting or accessing credit reference bureaus. This was meant to ensure digital borrowers, who are poor predominantly, are not precluded from accessing affordable loans due to poor credit histories.

7 Tavneet S, Paul G, 'How is digital credit changing the lives of Kenyans? Evidence from an evaluation of the impact of M-Shwari'< https://s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2018/10/23160405/Mshwari-Briefs-10-23-18-1.pdf > on November 4 2020.

8 FSD and CBK, 'FinAccessSurvey'.

9 -< https://egm.financedigitalafrica.org/> on November 2020.

10 Wamalwa P, Rugiri I and Lauler J, 'Digital Credit, Financial Literacy and Household Indebtedness'KBA 2019 <https://www.kba.co.ke/downloads/WPS-08-2019.pdf>

11 -< https://egm.financedigitalafrica.org/> on November 2020.

12 James H, William J, 'High Hopes: Experimental evidence on saving and the transition to High School in Kenya' < https://www.poverty-action.org/sites/default/files/publications/WP004_Habyarimana.Jackv3%20%281%29.pdf> on 4 November 2020.

13 MicroSave Consulting 'Making digital credit truly responsible' September 2019. https://www.microsavenet/wpcontent/uploads/2019/09/Digital-Credit-Kenya-Final-report.pdf > 4 November 2020.

14 Taylor L, Martin A, Sharma G and Jameson S (eds), Data Justice and COVID-19: Global Perspectives, Meatspace Press, 2020.

15 Central Bank, ' Review of emergency measures to facilitate Mobile Money Transactions' 24 June 2020<https://www.centralbank.go.ke/uploads/press_releases/913082204_Press%20Release%20-%2Review%20of%20Emergency%20Measures%20-%20Mobile%20Money%20Transactions.pdf > 4 November 2020.

Literature has now established that application of digital technologies to social problems is not a panacea to equity. It could either contribute to equity or exacerbate existing inequality.[16] For example, in response to the CBK directive suspending digital lending apps from the credit information-sharing system, digital lending apps immediately suspended customer credit limits.[17] For return customers, the credit apps typically expand or reduce their loan limits depending on how well they have honoured the terms of their loans. Some customers had progressively expanded their credit limits as a result of timely repayments. They were therefore surprised to find that they either could not borrow or could only borrow a small amount. This action by the apps demonstrates some of the problems with digital lending. As their business model depends on information, they argued that they could not continue dispensing loans without the assurance from credit information-sharing services.[18] However, since most of their customers are unaware of the factors that the apps consider when issuing them with loans, they felt unfairly treated when their loan limits were arbitrarily suspended or terminated. In this scenario, there was no direct authority to whom the customers could complain to.[19]This calls for analysis of how privacy and data protection are incorporated into fintech.

From a data perspective, fintech has been linked to rollout of digital ID by states. Actors such as the World Bank and the World Economic Forum (WEF) view digital ID as a catalyst for financial inclusion.[20] Closer home, Breckenridge relates the evolution of digital ID in Kenya to the need for a credit-sharing mechanism to support digital lending.[21] Research by Privacy International shows the how data intensive the financial sector is. It explores financial identity, a concept that supports practices such as electronic Know Your Customer (eKYC) and unique personal identifiers (UPIs).[22] Through digital ID, financial lenders can share data on people's financial habits, making it easier to issue loans backed by historical data.

National digital ID projects have been the subject of litigation for, among other things, excluding vulnerable populations from vital services as well as limiting the right to privacy.[23] In a case challenging Huduma Namba, the petitioners argued that it locks out those who have histori-

16 Taylor L, 'What is data justice? The case for connecting digital rights and freedoms globally' 4 Big Data and Society 2, 2017

17 Wambu W, 'Tough times ahead as mobile lending apps freeze loans' The Standard, 7 April 2020 <https://www.standardmedia.co.ke/business/article/2001367146/tough-times-ahead-as-mobile-lending-apps-freeze-loans> on 18 December 2020.

18 DLAK 'Submission on the Central Bank of Kenya (CBK) Amendment Bill 2020 - proposed amendments to bring the Digital Lending industry (DLI) under CBK Regulation' September 2020.

19 Wambu W, 'Tough times ahead as mobile lending apps freeze loans'

20 WEF, 'A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity' [2016] World Economic Forum 1.< http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf > on 4 November 2020.

21 Keith B, 'The Failure of the 'single Source of Truth' about Kenyans: The NDRS, Collateral Mysteries and the Safaricom Monopoly' 78.

22 Privacy International 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector'[2017] <https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf> on 7 Jan 2021

23 Caribou Digital.

cally been denied documents such as birth certificates and national identity cards.[24] They narrated the difficulties faced by these groups in what are considered normal processes for the average Kenyan (for example acquiring a phone number), and prayed for a digital ID system that prioritises the marginalised. Another argument was that Kenya did not have adequate privacy and data protection laws to assure the security and integrity of data collected from the project. The DPA was passed in the course of the petition, giving the Huduma Namba project a lifeline.

There are several studies demonstrating how fintech impacts privacy and data protection.[25] This can be traced to mandatory SIM card registration which increased the identifiability of data on mobile money transactions, leading to the growth of an economy created from personal data.[26] Privacy in welfare programs has also been studied widely in India, which has the world's largest digital ID system, *Aadhar.* In Africa, Carmona discussed a cash transfer programme involving social welfare grants in South Africa where social welfare recipients data was repurposed for marketing by a third party company linked to the private company involved in disbursement of the funds.[27]The study brings to light less obvious hazards to privacy in public funded but privately executed welfare programmes.

This study contributes to the strand on digital identities and fintech from a data protection perspective. It advances research by CIPIT partners, Privacy International on data privacy practices by financial institutions, particularly digital lending apps. It explores questions around the nature of data collected by fintech apps and privacy practices in response to the DPA.

24 *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others (Interested Parties) (2019) eKLR.*

25 See for example, Privacy International, 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector' [2017] <https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf> on 7 January 2021.

26 Keith B, 'Failure of a single source of truth'

27 Carmona M S, 'Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection' [2018] Extension of social security <https://www.ilo.org/secsoc/information-resources/publications-and-tools/Workingpapers/WCMS_631504/lang--en/index.htm>.

3. THE DPA AND DIGITAL LENDING APPS

3.1 Data Protection Principles

Digital lending apps are subject to the DPA since they involve processing of personal data. As shall be illustrated in the section on permissions, the apps access various types of data such as phone identity, messages on the phone, network connections, phone storage as well as location.

The DPA sets out principles that persons processing data must adhere to. These include protecting the privacy of data subjects, processing data in a lawful, fair and transparent manner as well as providing a valid explanation to the data subject for data processed. There are also several limitations on data practices including on purpose, adequacy and retention. Further data controllers and processors must keep accurate data and provide means through which data subjects can request for correction or deletion of inaccurate data. In addition, data can only be transferred outside Kenya to countries with adequate data protection frameworks. The following table summarises the data protection principles and their application to digital lending apps.

Table 1: Data protection principles and digital lending apps

Principle	Application
Right to privacy - Section 25(a)	Everyone has a right to be protected from unnecessary disclosure of their private and family affairs. Taking up of loans is a private affair that should not be disclosed.
Lawful, fair and transparent processing- Section 25(b)	Digital lending apps should disclose what information is gathered from the apps and how it is processed. Information gathered should also be pursuant to either a law or legitimate purpose, which in the case of digital lending could be credit scoring and keeping business records.
Purpose limitation- Section 25(c)	Borrowers should be provided with information on the purposes for which their information is collected. Digital lending apps should not repurpose the information they have without informing and obtaining the borrower's consent.
Adequacy limitation - Section 25(d)	Digital lenders should only process data that is relevant and sufficient for their purpose(s). They have access to data that is volunteered by the borrower at the registration stage, data that is gathered by the app through access to the borrower's smartphone, as well as data that is inferred from analysing the first two types of data.
Valid explanation - Section 25(e)	Digital lenders determine creditworthiness by analysing phone data, access personal data on the borrower's family and private affairs. They should therefore give a valid explanation as to why the family and private information is required.
Accuracy - Section 25(f)	Digital lenders should keep accurate information on borrowers. This includes promptly updating their repayment histories on credit-sharing information system.
Retention limitation -Section 25(g))	Digital lenders should not keep data perpetually. Digital lending apps should inform their customers how long their data, including inferred data, is kept and for what purposes.
Transfer outside Kenya -Section 25(h)	The DPA requires protection for personal data being transferred outside the country.

3.2 Other relevant provisions of the DPA

Other relevant provisions of the DPA relate to; the rights of data subjects, direct collection of data from the data subject, notification requirements, data protection impact assessment (DPIA), automated decision-making; data portability, and data protection by design and default.

3.2.1 Rights of the data subject

Borrowers on digital apps are data subjects with the right to be informed about the way in which their data will be used.[28]They also have a right to access their personal data held by the lender and, in some instances, can object to processing of part of their data.

3.2.2 Collection of data from the data subject

Section 27 envisages that data shall be collected from the data subject directly. However, digital lending apps also gather and infer data from the borrower's smartphone and other sources. Any other collection is subject to consent of the data subject. The DTA defines consent as the 'manifestation of express, unequivocal, free, specific and informed' agreement by the data subject.[29] Digital lending apps collect data through inference, which is not clear to many consumers.

3.2.3 Notification and information

The DTA envisages various situations where the data processor or controller is required to notify the data subject about processing activities.[30] Under this scheme, data subjects should be informed about their rights, the purposes for data collection, third parties with whom the data is will be shared, contacts of any entity that may receive the data, description of organisational and security measures taken to ensure integrity of the data, data collection that is mandatory and that which is voluntary, and the consequences where the data subject does not provide some of the data.

3.2.4 DPIA

The DPA subjects data processing activities that are likely to have a high risk on the rights of data subjects to an assessment of such risks and their mitigation.[31] DPIAs on digital lending apps also relate to consumer rights such as reasonable quality of services, consumer information and protection of health, safety and economic interests as they demand of the data processor a systematic analysis of all the principles of data protection in relation to their processing activity.

28 Section 26, DPA.

29 Section 2, DPA.

30 Section 29, DPA.

31 Section 31, DPA.

3.2.5 Protection from automated decision-making

The DPA protects data subjects from decisions based solely on automated processing.[32] Automated processing in digital lending includes profiling of the data subject during credit-scoring[33] and possibly listing of defaulters with credit reference bureaus. Digital lenders determine credit worthiness through analysis of the borrower's phone data using technologies such as algorithms to set loan limits, and in some cases, interest rates, repayment periods and penalties.[34]

3.3.6 Data portability

This is the right of a data subject to receive data about them in a meaningful format to enable its further use.[35] Ideally, digital lenders should be able to provide their borrowers reports and analyses with which they can move to other lenders. A person who has been borrowing from one lender should be able to move to another lender without having to start a fresh profile.

3.3.7 Data protection by design and default

The data protection framework requires data controllers to design products that incorporate data protection principles. In the event that the products were designed prior to the law, they should be reconsidered, and protection safeguards added to ensure that the products protect and promote privacy.[36]

32 Section 35, DPA.

33 Privacy International, 'Fintech: Privacy and Identity in the new data-intensive financial sector' November 2017. <https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector > on 4 November 2020.

34 For a more comprehensive list of technologies, see, Privacy International 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector'[2017] 11 <https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf> on 7 Jan 2021.

35 Section 38, DPA, 2019.

36 Section 41, DPA.

4. THE STUDY

The study seeks to understand the privacy practices of digital lending apps by analysing their privacy and data protection practices generally. It more specifically delves into a particular aspect – their sharing of data with third parties. Each of these steps, together with the challenges faced in the study, is briefly explained below.

4.1 Methodology

Once we had established the legal framework applicable to digital lending apps, we selected a few apps for the study. We analysed the privacy policies these apps and noted their data sharing policies. We also used a proxy tool to determine data collected by the apps at start-up.

4.1.1 Apps selection

Data collection began by identifying a sample of the leading digital lending apps in operation in Kenya[37] on Google Play Store, where majority of smartphone users source their apps. The study narrowed down to seven apps guided by the following criteria, whether: The app formed part of the top ten digital lending apps in operation at the commencement of the study;

a) The app was operational within Kenya; and

b) The app was downloadable from the Google Play Store, thus operational on android phones, which are widely available in Kenya.

Eventually, we studied seven apps, as summarised in Table 2. We established their registered ownership and also noted whether the app was deposit taking, therefore regulated by CBK or non-deposit taking.

Table 2: List of digital lending apps studied

App	Ownership	Type
Tala	InVenture Mobile Limited, registered in California	Non-deposit taking
Branch	Branch International, registered in California	Non-deposit taking
Okash	Opera, registered in Norway, with significant Chinese investors[38]	Non-deposit taking
KCB	KCB Group, registered in Kenya, regulated by CBK)	Includes banking services, savings and loans
Equity (Eazzy Banking)	Finserve Africa, a subsidiary of Equity Bank,	Includes banking services, savings and loans
Timiza	Absa Group, regulated by CBK	Includes banking services, savings and loans
Lioncash	Glora Tech Limited, registered in Kenya	Non-deposit taking

37 Mobile App Ranking < https://www.similarweb.com/apps/top/google/store-rank/ke/finance/top-free/ > on 17 June 2020.

38 Kazeem Y, 'The latest marker of Chinese interest in African fintech is a $120 million funding round for OPay' Quartz, 18 November 2019.

4.1.2 App permissions

The study sought to understand what data is accessed as well as other issues around the data, for example, how often it is accessed, and who accesses it. To analyse data handling, we listed the permissions that each app requires at installation. We also analysed the privacy policies of all the apps and listed the data-sharing policies.

4.1.3 Trackers

To study whether the apps shared user data collected by the trackers with third-party services, we set up the Fiddler proxy server tool with a physical device (Google Pixel) to collect the data by intercepting the web traffic. We were able to collect some data regarding the application programming interface (API) endpoints the applications were sharing data with, on application start.[39] We compared the data collected with existing privacy studies such as Exodus Privacy.[40]

4.2 Challenges And Limitations

The main challenges faced were i) selection of a traffic-monitoring methodology that is acceptable legally, and ii) unavailability of appropriate phones for the study locally.

4.2.1 Legality of traffic monitoring

Analysis of the actual data that digital lending apps access and share with third parties, if any, requires interception of the traffic being sent from the app to the third party server. Interception is outlawed under the Kenya Information and Communications Act (KICA)[41] as well as the Computer Misuse and Cybercrimes Act (CIMA)[42]. While the DPA[43] envisages research as a basis for processing data, such data processing has to be done by a data owner or on authorisation by the owner. Digital lending apps consider the apps their property. Some explicitly prohibit interception of traffic. We were therefore limited to monitoring the servers that the apps connect to at start-up and could not probe further what data the third party servers access.

39 Set up guide can be found here:https://www.telerik.com/blogs/how-to-capture-android-traffic-with-fiddler.

40 -< https://exodus-privacy.eu.org/en/ > on 17 June 2020.

41 Section 31, KICA.

42 Section 17, CIMA.

43 Sections 52 and 53, DPA.

4.2.2 Unavailability of appropriate phones for the study locally

Another challenge faced was in obtaining a phone that could carry out technical analysis. The most popular and widely used phones in the country are from the company Transsion Holdings. These include the brands Tecno, Itel and Infinix. Other popular brands are Oppo, Huawei and Xioami. These phones, it turned out, could not be rooted and therefore could not be studied using the man-in-the-middle (MITM) software.[44] The technical team therefore decided to use Google Pixel, which is friendlier to developers. However, this phone had to be sourced abroad, which delayed the study.

An issue noted with the popular phones was that they had pre-installed apps which a user cannot uninstall. These are popularly known as bloatware, due to the space and resources they occupy in the smartphone. It was not clear from the study whether there is any relationship between the bloatware and digital lending apps, and this was marked as an issue for further study.

44 --<https://privacyinternational.org/node/2732> on 9 January 2021.

5. DATA COLLECTION

5.1 App permissions

The study gathered data on permissions that digital lending apps require on installation for seven apps as shown in Table 3 below.

Table 3: Summary of permissions required by the apps

Permissions	Tala	Branch	OKash	KCB	Equity (Eazzy Banking)	Timiza	Lioncash
Phone	Read phone status and identity	Read phone status and identity	Read phone status and identity	Call phone numbers directly Read phone status and identity	Read phone status and identity	Call phone numbers directly read phone status and identity	
Contacts	Find accounts on the device Read your contacts	Read your contacts	Find accounts on the device	Read your contacts	Find accounts on the device Read your contacts	Read your contacts	Read your contacts
Device ID and call information	Read phone status and identity			Read phone status and identity	Read phone status and identity	Read phone status and identity	
Photos/ Media/ Files	Read the contents of your USB storage Modify or delete the contents of your USB storage				Read the contents of your USB storage Modify or delete the contents of your USB storage	Read the contents of your USB storage Modify or delete the contents of your USB storage	
Calendar	Read calendar events plus confidential information		Add or modify calendar events and send email to guests without owners knowledge Read calendar events and details				

Device and app history	Retrieve running apps Read your Web bookmarks and history		Retrieve running apps			Retrieve running apps	
SMS	Receive text messages (SMS) Read your text messages (SMS or MMS)	Receive text messages (SMS) Read your text messages (SMS or MMS)	Receive text messages (SMS) Read your text messages (SMS or MMS)				Read your text messages (SMS or MMS)
Camera	Take pictures and videos	Take pictures and videos		Take pictures and videos	Take pictures and videos	Take pictures and videos	
Identity	Find accounts on the device				Find accounts on the device		
Location	Approximate location (network-based) Precise location (GPS and network-based)	Approximate location (network-based) Precise location (GPS and network-based)	Approximate location (network-based) Precise location (GPS and network-based) Access extra location provider commands	Approximate location (network-based) Precise location (GPS and network-based)	Approximate location (network-based) Precise location (GPS and network-based)	Approximate location (network-based) Precise location (GPS and network-based)	Approximate location (network-based) Precise location (GPS and network-based)
Wi-Fi connection information	View Wi-Fi connections	View Wi-Fi connections	View Wi-Fi connections		View Wi-Fi connections	View Wi-Fi connections	View Wi-Fi connections
Storage	Read the contents of your USB storage Modify or delete the contents of your USB storage	Read the contents of your SD Card Modify or delete the contents of your SD Card	Read the contents of your SD Card Modify or delete the contents of your SD Card	Read the contents of your USB storage Modify or delete the contents of your USB storage	Read the contents of your USB storage Modify or delete the contents of your USB storage		Read the contents of your SD Card Modify or delete the contents of your SD Card

Micro-phone		Record audio					
Others	Receive data from Internet	Appear on top of other apps	Appear on top of other apps	Receive data from Inter-net	Receive data from Inter-net	Receive data from Inter-net	Connect and disconnect Wifi
	View network con-nections	Run at start-up	Run at start-up	Full network access	View net-work con-nections	View net-work con-nections	Have full net-work access
	Draw over other apps	Prevent phone from sleeping	Have full network access	Prevent device from sleeping	Full network access	Connect and disconnect Wi-Fi	View net-work connec-tions
	Change network connectivity	Receive data from the internet	View net-work con-nections	View net-work con-nections	Control vibration	Full network access	Prevent phone from sleeping
	Run at start-up	Control vibration	Retrieve running apps	Control vibration	Prevent device from sleeping	Run at start-up	Play Install Referrer API
	Pair with Bluetooth devices	Have full network access	Prevent phone from sleeping	Read Google service con-figuration	Read Google service con-figuration	Control vibration	Receive data from the internet
	Prevent device from sleeping	Play Install Referrer API	Play Install Referrer API			Prevent device from sleeping	
	Create accounts and set passwords		Receive data from Internet				
	Use accounts on the device						
	Control vibration						
	Full network access						

5.1.1 Discussion

All the apps read contacts, location data and have access to network connectivity data. This could be for purposes of geo-locating the loans to Kenya. However, the apps have continuous access to location data, meaning that they track borrowers' movements. Notably, Okash requires an extra location permission - 'access extra location provider commands'. Coupled with the fact that the apps run at start-up and prevent the phone from sleeping, this raises issues from a data protection perspective, for example, transparency and data minimisation. Does a loan app need to study borrowers' movements constantly? To what other use is such location data put?

Other permissions that raise data protection concerns include Branch's requirement to access the borrower's phone microphone in order to record audio as well as Okash's access to the calendar, which includes the permission to add or modify calendar events and email guests without the borrower's knowledge. Most of the apps read phone status and identity and text messages on the phone. As with other permissions, this was not a one-off permission required during installation, but constantly required.

Three apps, Branch, Okash and Lioncash, use referrer APIs. An install referrer is described as 'an identifier unique to Android devices which enables marketers to attribute ad activity to media sources for Google Play Store apps'.[45] This means that data on borrowers who install the lending apps from other pages or apps is also recorded.

5.2 Digital lending apps and third-party data-sharing

In pursuing the question of what other uses the data collected by digital lending apps was put to, the study attempted to find out whether digital lending apps share borrowers' data with third parties and if so, which ones.

In their privacy policies, all the lending apps disclosed that they share certain data with third parties, for example, for purposes of verifying identity, and in the normal course of business. Table 4 summarises how the privacy policies of the various apps address data-sharing with third parties.

45 Neto M ' Google Play Reffer API: Track and measure your app installs easily and securely' 20 November 2017 < https://android-developers.googleblog.com/2017/11/google-play-referrer-api-track-and.html > 4 November 2020.

Table 4: Summary of policies on third party data-sharing by the apps

	On the app (during installation)	On online privacy policy	On use of trackers (from privacy policy)
Tala[46]	Verify your identity through our secure system	Borrower data may be transferred to third parties like: · Tala and Tala sub-contractors; · persons acting on behalf of the borrower; · companies such as payment recipients, beneficiaries, account nominees, intermediaries, correspondent and agent banks, clearing houses, clearing or settlement systems, market counterparties, upstream withholding agents, swap or trade repositories, and stock exchanges; · purchasers of Tala (in case of sale); · credit reference bureaus · third parties to whom Tala provides referrals; · third party business operators in functions like transaction processing, fraud prevention, and marketing; · law enforcement agencies; and · any other service permitted by law.	Tala explains that it uses trackers to 'to distinguish you from other users of the app, app site or service Site'

46 Privacy Policy < https://tala.co.ke/privacy-policy-ke/ > on 4 November 2020.

Branch[47]		Instances where borrower data may be disclosed to third parties are listed as: · in case of sale of the business; · in case of selling of assets, where customer data is one of the assets sold; · in response to a legal or compliance request; · in enforcing Branch's terms and conditions; · in investigating potential breaches; · in reporting defaulters to any credit bureau; and · for the purpose of publishing statistics relating to the use of the app.	Branch uses trackers to 'to distinguish you from other users of the app, app site or service site'
OKash [48]	Verification of identity Verification of Mpesa number Verification of emergency contact	Okash lists the following as third parties with whom borrower's data may be shared: · credit bureaus, in requesting credit histories or reporting loan defaults; · collections agencies, in seeking to collect overdue loans; · Government bodies and law enforcement agencies, to comply with the law; · professional advisers, to enforce or defend legal rights; or · purchaser or seller in connection with a corporate event such as a merger, business acquisition or insolvency situation.	Not stated.

47 Privacy Policy < https://branch.co.ke/pp > on 4 November 2020.

48 Privacy policy < https://ke.o-kash.com/kenya/en/privacy-policy/> on 4 November 2020.

KCB[49]	Verification of identity	KCB lists that they may share information: · with third parties to whom they assign their rights; · with other companies that are part of the KCB group including for marketing purposes. · for purposes of ongoing or proposed contracts; · during account opening, when information is shared with other companies in the group for credit-scoring, credit reference, fraud prevention, insurance, and debt tracing etc; · with agents regarding how a data subject manages their account; · when compelled by law; · with the customer's consent; and · when it is in KCB's interest to do so.	KCB may use borrowers' information for 'assessment and analysis (including credit and/or behaviour scoring, market and product analysis).'
Equity	Verification of identity	Among parties to whom information may be disclosed include: · companies that are members of Equity Group; · business partners, suppliers and sub-contractors for the performance a contract; · Advertisers and advertising networks that require the data to select and serve relevant ad-verts to the data subject and others (without disclosing identifiable information); · agents; · Government and enforcement agencies; and · Credit and other payment card companies and screening companies.	Equity may 'analyze and use the information we have to evaluate and improve our services, research, develop, and test new services and features, and conduct trouble-shooting activities.'

49 Privacy Policy < https://kcbgroup.com/privacy-policy/> on 4 November 2020.

Timiza[50]	Verifying your identity	Absa Group, which owns Timiza, lists the following cases for disclosure to third parties: · with members of Absa Group as well as service providers; · parties to whom Absa assigns its rights; · local and global regulatory authorities; and · credit reference agencies for purposes of ascertaining credit worthiness.	Not mentioned.
Lioncash[51]	Verify your identity	Lioncash has a long list detailing how borrowers's data is used. The main headings include: · contractors hired to perform services such as collection services, background investigation, and skip tracing; · third parties that provide products and services; · good faith disclosures (such as:to comply with a law, regulation, court order, or other legal process; to detect, prevent, and respond to fraud, intellectual property infringement, violation of contracts or agreements, violation of law, or other misuse of LionCash Internet sites, apps, products or services; to protect LionCash rights or property or the data subject's or others' health, safety, welfare, rights, or property; or under similar circumstances); · in case of a business sale; and · credit reference bureaus.	Lioncash may share information with business partners for purposes of marketing as well as learning how borrowers interact with the app.

50 Terms of Service <https://www.absabank.co.ke/content/dam/kenya/absa/pdf/Terms-of-use/timiza-account-terms-and-conditions.pdf > on 4 November 2020.

51 Privacy Policy < http://lioncash.co/privacy-policy/ > on 4 November 2020.

5.2.1 Discussion

All the apps inform borrowers that the verification of their identity or phone numbers is carried out. For Okash, the verification includes the emergency contact declared by the borrower. It appears that the verification happens outside the apps, although apps such as Tala disclose that they store the data in their system. The verification involves back-linking with Government and private digital ID databases. For example, the apps use the Integrated Population Registration Services (IPRS) system to verify the borrower's national ID number. Some, such as Okash, also explain that they verify the phone number using the mobile network operator systems. This illustrates the inter-linkage between public and private identity systems.

All the apps also state that they share data with credit reference bureaus. Notably, at the onset of the COVID-19 pandemic, the CBK withdrew approvals given to 'digital (mobile-based) and credit-only lenders as third-party credit information providers to CRBs'.[52] This means that non deposit taking apps such as Tala, Branch, Okash and Lioncash can no longer share information with credit reference bureaus. The effect of the withdrawal from the system was that digital lending apps immediately suspended loan limits for their borrowers. For example, borrowers who had built positive credit profiles by repaying their loans on time and therefore being eligible for higher loans were suddenly unable to get their loans within their limits or any loans at all.[53] Digital lenders argued that since their loans are backed, not by deposits but investments, investors had to be consulted over the new changes. However, the decision was made without consultations with customers, raising questions of transparency in data processing.

Notably, while some of apps disclosed that they study borrower behaviour for purposes of marketing, none of them explained that they share data with third-parties that engage in data analysis. In the next section, this study attempts to establish whether the apps connect with data analytic companies that are also known to sell ads.

5.3 Checking data on trackers

The third point of data collection was to check for trackers. A tracker may be defined as 'a piece of software meant to collect data about you or your usages.'[54] There are various types of trackers such as crash reporters, which inform the app company about performance outages, analytics that collect data about how the customer uses the app, profiling that collects data about the app user's behaviour, ads that serve targeted ads to the customer as well as location trackers that determine the geographical location of the phone where the app is installed.

To learn the trackers used by the seven apps, the study collected data on API endpoints the applications were sending data to, on application start. Table 4 is a summary of the data collected.

52 Central Bank, 'Publication on the credit reference bureau regulations, 2020 and additional measures on credit information sharing' 14 April 2020 < https://www.centralbank.go.ke/uploads/pressreleases/850440997_Press%20Release%20-%20Credit%20Reference%20Bureau%20Regulations%20-%20April%202020.pdf > on 4 November 2020.

53 Milcah K, ' The Central Bank of Kenya (CBK) Amendment Bill (2020): A reflection on the public discussion on unlocking regulation of digital lenders' August 19,2020 < https://cipit.strathmore.edu/the-central-bank-of-kenya-cbk-amendment-bill-2020-a-reflection-on-the-public-discussion-on-unlocking-regulation-of-digital-lenders/ > on 4 November 2020.

54 -< https://reports.exodus-privacy.eu.org/en/info/trackers/ > on 4 November 2020.

Table 5: Summary of connections at start-up

App	Connect	Host	Connection	User agent
TALA	app.adjust.com:443 HTTP/1.1	app.adjust.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	taukibreez.iad-03.braze.com:443 HTTP/1.1	taukibreez.iad-03.braze.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	app.adjust.net.in:443 HTTP/1.1	aapp.adjust.net.in:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	api.amplitude.com:443 HTTP/1.1	api.amplitude.com:443	Keep-Alive	okhttp/3.12.8
	prod-ke-auth.inventureaccess.com:443 HTTP/1.1	prod-ke-auth.inventure-access.com:443	Keep-Alive	okhttp/3.12.8
	firebaseremoteconfig.googleapis.com:443 HTTP/1.1	firebaseremoteconfig.googleapis.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	userlocation.googleapis.com:443 HTTP/1.1	userlocation.googleapis.com:443		grpc-java-okhttp/1.34.0-SNAPSHOT
BRANCH	userlocation.googleapis.com:443 HTTP/1.1	userlocation.googleapis.com:443		grpc-java-okhttp/1.34.0-SNAPSHOT
	api.amplitude.com:443 HTTP/1.1	api.amplitude.com:443	Keep-Alive	okhttp/3.12.8
	graph.facebook.com:443 HTTP/1.1	graph.facebook.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	firebaseinstallations.googleapis.com:443 HTTP/1.1	firebaseinstallations.googleapis.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	branch.co:443 HTTP/1.1	branch.co:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	android.clients.google.com:443 HTTP/1.1	android.clients.google.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	conversions.appsflyer.com:443 HTTP/1.1	conversions.appsflyer.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	notify.bugsnag.com:443 HTTP/1.1	notify.bugsnag.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
OKASH	firebaseinstallations.googleapis.com:443 HTTP/1.1	firebaseinstallations.googleapis.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)

	service.ke.o-kash.com:443 HTTP/1.1	service.ke.o-kash.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	userlocation.googleapis.com:443 HTTP/1.1	userlocation.googleapis.com:443		grpc-java-okhttp/1.34.0-SNAPSHOT
KCB	kcbgroup.com:443 HTTP/1.1	kcbgroup.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	infinitedata-pa.googleapis.com:443 HTTP/1.1	infinitedata-pa.googleapis.com:443		grpc-java-okhttp/1.34.0-SNAPSHOT
	superapp.kcbbankgroup.com:9447 HTTP/1.1	superapp.kcbbankgroup.com:9447	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
Equity(Eazy Banking)	graph.facebook.com:443 HTTP/1.1	graph.facebook.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	api.branch.io:443 HTTP/1.1	api.branch.io:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	firebasestorage.googleapis.com:443 HTTP/1.1	firebasestorage.googleapis.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
TIMIZA	graph.facebook.com:443 HTTP/1.1	graph.facebook.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	play.googleapis.com:443 HTTP/1.1	play.googleapis.com:443	Keep-Alive	com.google.android.gms/204516019 Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
LION-CASH	graph.facebook.com:443 HTTP/1.1	graph.facebook.com:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)
	firebase-settings.crashlytics.com:443 HTTP/1.1	firebase-settings.crashlytics.com:443	Keep-Alive	okhttp/3.12.1
	zeus.lioncash.co:443 HTTP/1.1	zeus.lioncash.co:443	Keep-Alive	Mozilla/5.0 (Linux; Android 8.1.0; Pixel Build/OPM1.171019.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.198 Mobile Safari/537.36
	scontent.fnbo10-1.fna.fbcdn.net:443 HTTP/1.1	scontent.fnbo10-1.fna.fbcdn.net:443	Keep-Alive	Dalvik/2.1.0 (Linux; U; Android 8.1.0; Pixel Build/OPM1.171019.011)

The study analysed the API endpoints that the apps were connecting to. Table 6 shows a summary of these findings.

Table 6: Description of endpoints that APIs apps are connecting to

Domain	Sub-domain	Services
adjust.com	app.adjust.com	Connects and analyses cross-platform data.
		Discovers where best users come from.
		Targets, advertises and optimizes information for most valuable users.
braze.com	taukibreez.iad-03.braze.com	Braze provides a high-performance REST API to allow you to track users, send messages, export data, and more.
amplitude.com	api.amplitude.com	Amplitude is used to user actions to help digital product and growth teams instantly understand user behaviour, build engaging experiences, and grow their business.
googleapis.com	firebaseremoteconfig.googleapis.com, userlocation.googleapis.com, firebaseinstallations.googleapis.com, firebasestorage.googleapis.com, play.googleapis.com, infinitedata-pa.googleapis.com	Google APIs are application programming interfaces developed by Google, which allow communication with Google Services and their integration to other services.
facebook.com	graph.facebook.com	The Graph API is the primary way for apps to read and write to the Facebook social graph.
appsflyer.com	conversions.appsflyer.com	Data tracking.
bugsnag.com	notify.bugsnag.com	Bugsnag monitors application stability so you can make data-driven decisions on whether you should be building new features, or fixing bugs.
branch.io	api.branch.io	Branch Metrics provides solutions that unify user measurement across different devices, platforms, and channels.
fbcdn.net	scontent.fnbo10-1.fna.fbcdn.net	The Facebook Content Distribution network 'delivers photos and videos to people who use Facebook'. It contains multiple layers and caches.
google.com	firebase-settings.crashlytics.com, android.clients.google.com	Analytics.
adjust.net.in	aapp.adjust.net.in	UNKNOWN, Adjust is a mobile measurement company.
inventureaccess.com	prod-ke-auth.inventureaccess.com	UNKNOWN. Inventure is Tala's registered company name.
branch.co	UNKNOWN	Website for branch app.
o-kash.com	service.ke.o-kash.com	Okash api service
kcbgroup.com	UNKNOWN	Website for branch KCB.
kcbbankgroup.com	superapp.kcbbankgroup.com	UNKNOWN but connected to KCB group.
lioncash.co	zeus.lioncash.co	UNKNOWN but connected to KCB group.
crashlytics.com	firebase-settings.crashlytics.com	Redirects to firebase.google.com

5.3.1 Discussion

The data above shows the information exchanged between the apps and the host at start-up. The data is evidence of the apps connecting to different types of trackers such as the app companies' servers, crash reporters, analytics and location data. For example, Tala, KCB and Equity all connect to location data through the Google user location API. Generally, non-deposit taking apps, gather more data compared to apps that offer other banking services.

The apps connect to those tracking services every time the app is launched. For example, http://userlocation.googleapis.com:443 ensures that the app will always have the user's location data, which could be used for unsolicited advertising. api.amplitude.com:443 HTTP/1.1 tracks deleted accounts, indicating that borrowers' data is tracked even for services they may have opted out of.

Evidence indicates linkages to third-party APIs include the Facebook graph API, which is the primary means of getting data in and out of Facebook. Four of the apps, API,[55] Branch, Equity, Timiza and Lioncash connected to the API at start-up.

The data also indicates connection to Bespoke data analytics companies which study user behaviour and sell targeted ads. The Adjust API found on Tala is a retargeting software, which studies user behaviour. According to their website, they help to target ads in real time through retargeting and exclusion targeting.[56] Braze, also found on Tala, is a targeted ad company. It describes itself as a mobile engagement platform that helps brands connect to consumers through data.[57] Another data analytics API is Amplitude,[58] which appeared on both Tala and Branch. Branch also connected to the analytics firm Appsflyer.[59]

Relating this data back to Tables 2 and 3 that list permissions required by the apps and disclosures about how data is shared with third parties respectively, the evidence of trackers leads us to several conclusions: -

a) digital lending apps are not only about giving loans to borrowers. The relationship extends to studying borrowers' behaviour. This is inferred from the evidence of trackers that constantly track borrower behaviour such as the Facebook API and user location.
b) digital lending apps share data obtained from studying borrowers with third parties such as data analytic companies who later use the data for marketing and ads. This is deduced from the evidence of apps connecting to data analytic companies such as Adjust, Amplitude and Braze.
c) The data aspect of digital lending apps is ubiquitous to the borrower as well as policy-makers and regulators. Hence, previous regulatory efforts have focussed on financial fairness, for example regulating interest rates and protecting borrowers from effects of negative listing on credit information-sharing systems. Regulating profiling of borrower data with third party data analytics and marketing companies has not been considered.

55 - < https://developers.facebook.com/docs/graph-api/overview/ > on November 2020
56 - < https://www.adjust.com/product/adjust-audience-builder/ > on November 2020
57 - < https://www.braze.com/ > on November 2020
58 - < https://amplitude.com/ > on November 2020
59 - < https://www.appsflyer.com/ > November 2020

5.4 Summary of findings

This study sought to understand the privacy and data protection practices of digital lending apps. From the analysis of the sampled digital lending apps, the study found that the apps do not comply with the provisions of the DPA. Table 7 below summarises the gaps between the practices of the apps and the DPA.

Table 7: Summary of gaps between the DPA and digital lending apps

DPA provision	Practices by digital lending apps
Right to privacy - Section 25(a)	The right to privacy extends to privacy of communications, yet the model of non-deposit taking loan apps depends on analysing personal data on the phone and making inferences such as a borrower's creditworthiness. This infringes on privacy.
Lawful, fair and transparent processing - Section 25(b)	Digital lending apps give financial information such as cost of loans in the app, even before it is downloaded. However, information on data aspects was not as explicit. For example, even where an app explains that it uses data on the borrower's phone to determine credit limits, the parameters used in determining creditworthiness are not known to borrowers. This was particularly evident after the COVID-19 pandemic when some of the apps abruptly suspended the system of loan limits.
Purpose limitation - Section 25(c)	As noted from Tables 5 and 6, some digital lending apps connect to well-known data analytic systems. While the study could not establish if the data is sold, it raises concerns that the data is used for purposes other than determining creditworthiness. Some banks send prospecting messages to would be customers, stating loan amounts they qualify for without disclosing how the loan limits were arrived at. This means that the banks use information collected or analysed from other sources. Such information is collected for other purposes, and may not be related to the purpose of prospecting for new customers.
Adequacy limitation - Section 25(d)	As shown in Table 4 on permissions required by the digital lending apps, the amount of data collected is vast. The granularity of data collected is also deep, raising questions as to how much behavioural information is required to determine creditworthiness. Coupled with the fairness principle, there are also questions on whether data needs to be collected continuously, or whether a good credit history could suffice. Notably, there is a credit information-sharing system from which stakeholders can access borrower's data.
Valid explanation - Section 25(e)	It was noted that the privacy policies as well as terms are all in the English language. None of the apps studied provided notices in local languages or in forms other than written terms posted on their websites.
Accuracy - Section 25(f)	Keeping accurate information on borrowers is of utmost importance in the digital loan contract. This is because credit information is shared with other stakeholders. Credit information sharing has a legal effect as it determines the borrower's credit profile not only within the particular lending app but also with other stakeholders such as banks. Therefore, wrong credit information could deny a borrower better terms in future.

Retention limitation - Section 25(g)	Digital lenders do not inform their customers how long their data, including inferred data, is kept, and for what purposes.
Transfer outside Kenya - Section 25(h)	The Google Play Store does not always identify the app owner sufficiently. While it may be easier for customers to recognise bank-owned apps, non-bank-owned apps are not always recognisable. Even where an app is owned by a Kenyan entity, this does not automatically mean that it stores data in Kenya or another country with adequate data protection laws.
Rights of the data subject - Sections 26 and 27	The right to correction or deletion of false or misleading data is very relevant in addressing the complaints about borrowers' repayments not being updated, or defaulters not being de-listed from credit reference bureaus once discharged.[<?>]
Collection of data from the data subject directly - Section 28	It can be inferred from Table 4 on permissions that communication from persons who do not have any relationship with digital lending apps is collected. This is possible when the apps read messages or other media in the borrowers' phone.
Notification - Section 29	The notification requirements are legal tools through which consumer information rights are respected. While there are digital lenders who provide these notifications through terms and conditions, it was noted that the privacy policies and terms are all in the English language. None of the apps studied provide notices in local languages or in forms other than written terms posted on their websites. In addition, not all the notifications are a one-time requirement. For example, sharing consumer data with third parties may occur when authorities or business partners seek business statistics. Borrowers should be notified when such third-party data-sharing occurs. In the event of a change of business ownership on the part of the lender, the borrowers should not only be informed, but also afforded an opportunity to object or restrict the processing of their data.
DPIA	None of the apps reviewed had a published DPIA. This may be because the DPA is novel, having come into force only a year ago. Digital lending apps should carry out comprehensive DPIAs since they process sensitive personal data.
Protection from automated decision-making - Section 35	The apps explain that they analyse data to determine creditworthiness - this is automated decision-making. However, they do not explicitly provide mechanisms for redress for borrowers aggrieved by automated decision-making.
Data portability - Section 38	The apps do not provide information on how one can port their data to another service provider. This calls for digital lenders to incorporate interoperability as part of their system design. The regulator should also intervene to ensure that borrowers are not locked to one lender. Data portability is one tool through which this may be achieved.
Data protection by design and default - Section 41	The digital lending apps do not protect and promote data protection by design. For example, they do not incorporate meaningful consent.[<?>] They also lack sufficient information on the types of data being collected. In addition, it is not disclosed to consumers how long their data is kept and who it is shared with. Further, there isn't enough communication or notification to consumers on processing that affects their interests.

5 A note on COVID-19 and digital lending apps

In response to the COVID-19 pandemic, the government gave directives aimed at enhancing cashless transactions and cushioning the poor from the effects of reduced economic activities.[60] Among these was the removal of non-deposit taking digital lending apps as credit information providers.[61] This effectively locked out non deposit taking apps from reporting defaulting borrowers in the credit reference information sharing system.

In response, non-deposit taking digital lending apps suspended loan for borrowers. They also suspended credit limits for customers who had built positive credit histories by borrowing and paying consistently on time.[62]Some of the user complaints noted from the Google App Store, as well as social media handles of digital lenders, point to a change of policies by the lenders as a result of COVID-19 and a lack of information on the policies. Borrowers and the public were not notified of these changes.[63]

Eventually, digital lenders through their association, Digital Lenders Association of Kenya (DLAK), announced that they would support the Government policy on restructuring loans[64] to assist borrowers that were facing difficulties as a result of the pandemic. [65]

6 CONCLUSION

The study found that the sample of seven digital lending apps in the study have all published privacy policies that attempt to align them with the DPA. However, as summarised in Table 7, the policies, combined with practices such as sharing data with third parties, do not comply with the DPA. On the particular issue of third-party data-sharing, the study found evidence of some of the apps having embedded trackers that profile user behaviour. This demonstrates the challenges of privacy and data protection as a means of regulating a business whose model depends on analysing personal data. It is compounded when data is shared with third parties that may process it for other purposes such as marketing and advertising. To remedy these problems, regulators need to expand their focus from financial aspects of digital lending apps to data aspects, including the principles under the DPA, and the issue of third party data-sharing.

60 --<http://kenyalaw.org/kenyalawblog/kenyas-response-to-covid-19/>

61 Central Bank of Kenya, 'Publication of the Credit Reference Bureau Regulations, 2020 and Additional Measures on Credit Information Sharing', 14 April 2020 <https://www.centralbank.go.ke/uploads/press_releases/850440997_Press%20Release%20-%20Credit%20Reference%20Bureau%20Regulations%20-%20April%202020.pdf> on 25 Jan 2021

62 Wambu W, 'Tough times ahead as mobile lending apps freeze loans' The Standard, 7 April 2020. <https://www.standardmedia.co.ke/business/article/2001367146/tough-times-ahead-as-mobile-lending-apps-freeze-loans> 18 Dec 2020.

63 -< https://www.linkedin.com/posts/alihkassim_neobanks-crb-socialdata-activity-6649660235399118848-Cok3/ > 4 November 2020.

64 Central Bank of Kenya, 'Banking Circular No. 3 of 2020: Implementation of the emergency measures to mitigate the adverse impact of corona virus (COVID-19) pandemicon loans and advances', 27 March 2020 <https://www.centralbank.go.ke/uploads/banking_circulars/1400484618_Banking%20Circular%20No.%203%20of%202020%20-%20Implementation%20of%20Emergency%20Measures.pdf> 25 Jan 2021

65 Wako A, 'Digital lenders unveil measures to guide sector during coronavirus crisis' Nairobian, 20 March 2020 <https://nairobinews.nation.co.ke/editors-picks/digital-lenders-unveil-measures-to-guide-sector-during-coronavirus-crisis>.

Strathmore University

Centre for Intellectual Property and Information Technology Law

Ole Sangale Rd, Madaraka Estate.
PO Box 59857-00200, Nairobi, Kenya.
Tel +254 (0)703 034612
Email: cipit@strathmore.edu
Website:www.cipit.strathmore.edu

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

REPORT BY GRACE MUTUNG'U AND KEVIN MUCHWAT

© 2021 by Center of Intellectual Property and Technology Law (CIPIT). This work is licensed under a Creative Commons Attribution – NonCommercial – ShareAlike 4.0 International License (CC BY NC SA 4.0). This license allows you to distribute, remix, adapt, and build upon this work for non – commercial purposes, as long as you credit CIPIT and distribute your creations under the same license: https://creativecommons.org/licenses/by-nc-sa/4.0/