A POUND OF FLESH FOR 3,000 DUCATS, AND SOME DATA: AN APPRAISAL ON THE ADEQUACY OF DATA PROTECTION LAW IN DIGITAL LENDING IN KENYA

***Augustus Mutemi Mbila*[160*]**

Abstract

Since the introduction of M-Shwari as a digital lender by Commercial Bank of Africa in 2012, the lending market has seen a proliferation of digital lenders that are largely unregulated. The lenders provide seemingly cheap loans whose interest is huge when the Annual Percentage Rate (APR) is calculated from the weekly, bi-weekly, or monthly payment requirements. The lenders operate through apps that are uploaded to App Stores and pulled down at will. They require their customers to 'accept' terms and conditions before accessing the loans, and these terms sometimes allow the lenders unfettered access to customer data which they use and abuse in equal measure. The lenders use such customer data to issue threats, to contact those on the contact lists of the customers' phonebook, and to report them on Credit Reference Bureaus (CRBs). Based on this mode of operation, these lenders have rightfully earned the name "shylocks".

Through the Central Bank of Kenya (Amendment) Act of 2020, the Central Bank of Kenya (CBK) has been empowered to regulate the activities of these digital lenders. However, this paper raises key concerns on such powers because the mode of operation of these digital lenders is such that the CBK may not adequately regulate them. Does the CBK have capacity to trace the uploading of the apps to App Stores to ensure that they have been uploaded there after obtaining the requisite license? What are the consequences of breach of data privacy and dignity of the customer by the digital lenders? Does the CBK have enough powers and capacity to protect consumers of these services from abuse by the digital lenders? The paper interrogates these issues within the relevant law and concludes that there is a lot more to be done as the available law is not adequate.

Keywords: Financial inclusion; Digital lending; Mobile Network Operators (MNOs); Annual Percentage Rate (APR); data; Data Protection.

160 *LL.B. (Hons) (University of Nairobi), LL.M. (Regional Integration and East African Community Law) - (University of Dar es Salaam and University of Bayreuth in Germany), PhD. (Candidate), Lecturer and Consultant in Law. The author can be reached on augumtemi@gmail.com for comments on this article.

1.0 Introduction

The need to boost financial inclusion in the Kenyan economy has led to the evolution and development of digital microcredit. Financial inclusion encompasses all initiatives taken to make formal financial services available, accessible and affordable to all segments of the population.[161] Traditional credit providers have: archaic, mundane and lengthy procedures as mandatory requirements for those looking for credit. This has made it almost impossible for borrowers to obtain credit from those providers. Digital microcredit therefore exists to fill in this gap. Digital lending has been defined as:

'[t]he process of offering loans that are applied for, disbursed, and managed through digital channels, in which lenders use digitized data to inform credit decisions and build intelligent customer engagement.'[162]

A report by Financial Sector Deepening (FSD) shows that by 2019, approximately 88% of the adult population in Kenya had access to mobile money and that over six million Kenyans had borrowed money from digital mobile lenders to meet their daily needs.[163] Since the introduction of M-Shwari in 2012, the number of mobile platforms providing quick access to loans has shot up to approximately 50 in 2019.[164] Available data shows that these digital lending platforms charge high interests for loans that must be paid within a very short time, sometimes within a week.[165] The Annual Pricing Rate (APR) sometimes shoots to 15 times the interest that commercial banks charge for unsecured loans. However, despite the high interest rates, borrowers still access these loans because of the ease of accessing them compared to the process they must undergo if they were to access the loans from commercial banks.[166] Defaulters are listed with the Credit Referencing Bureau (CRB), hence tainting their creditworthiness, despite the little amounts they might have borrowed.[167] The platforms also illegally and without consent access confidential data

161 Triki, T and Faye, I, 'Financial inclusion in Africa' *African Development Bank* 2013, 25 https://www.afdb.org/fileadmin/uploads/afdb/documents/Project-and-Operations/Financial_Inclusion_in_Africa.pdf accessed 21/09/2021.

162 Amy Stewart, Kathleen Yarowski, Paul Lamont, 'Demystifying Digital Lending; How Digital Transformation Can Help Financial Service Providers Reach New Customers, Drive Engagement, and Promote Financial Inclusion' *Accion Global Advisory Solutions*, 2018, 9 available at https://www.findevgateway.org/sites/default/files/publications/files/1123_digital_lending_r10_print_ready.pdf accessed 21/09/2021

163 FSD Kenya, "Digital credit audit report: Creating value through inclusive finance Evaluating the conduct and practice of digital lending in Kenya", Available at https://fsdkenya.org/publication/digital-credit-audit-report-evaluating-the-conduct-and-practice-of-digital-lending-in-kenya/ accessed on September 21, 2021.

164 See note 2, above.

165 Central Bank of Kenya (CBK), 'Kenya National Bureau of Statistics (KNBS) & FSD Kenya'. (2019). 2019 FinAccess household survey. Nairobi, Kenya. Available at https://www.centralbank.go.ke/uploads/financial_inclusion/2050404730_FinAccess%202019%20Household%20Survey-%20Jun.%2014%20Version.pdf , accessed on September 21, 2021.

166 FSD Kenya, 2018. 'Digital credit in Kenya: evidence from demand-side surveys'. Available at https://fsdkenya.org/publication/digital-credit-in-kenya-evidence-from-demand-side-surveys/, accessed on September 27, 2021.

167 Kaffenberger, Michelle, and Edoardo Totolo. 2018. 'A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania.' Working Paper. Washington, D.C.: CGAP.

from the borrowers, which in effect injures the borrowers' privacy rights.

Data protection and privacy is a constitutional right.[168] When digital lenders share their customer data to third parties, they infringe the constitutional right to privacy. The Data Protection Act[169] was enacted to give effect to article 31(c) and (d) of the Constitution on the protection of personal data.[170] It is however argued that the way digital lenders operate makes it difficult for this Act to adequately regulate digital lending and to protect the data of customers.

This paper attempts to examine the nature of digital lending in the country, the extent to which digital lending in Kenya is regulated and attempts towards protection of customer data.

2.0 The nature and status of digital lending in Kenya

Digital borrowers in Kenya account for approximately 54% by volume of yearly loans in Kenya. This market continues to grow, and it is estimated that this percentage will increase to approximately 60% by 2022.[171] Digital lending in Kenya now exists within three models. The first model is when Mobile Network Operators (MNOs) like Safaricom, Telkom, and Airtel collaborate with financial institutions to provide credit.[172] The creditworthiness of the customer is determined by complex formulae and algorithms designed by the credit providers. The borrower must be a customer of the MNOs for them to apply for credit. The most common examples of such collaborations in Kenya are Safaricom M-Pesa teaming up with Commercial Bank of Africa (CBA) to provide M-Shwari and Safaricom M-Pesa teaming up with the Kenya Commercial Bank (KCB) to provide KCB-Mpesa. The products are approved by the Central Bank of Kenya, which also allows the financial institutions to charge a facilitation fee.[173]

The second model is the mobile application-based model. The applications are designed and uploaded onto application stores for download by customers. The number of mobile apps providing instant, automated credit in the two main mobile app stores, Google Play and App Store keeps fluctuating. In 2018, there were approximately 110 such mobile apps on Google Play and App Store. However, 65 of these apps had been pulled down from the stores by April 2019, with 47 new ones emerging on the stores. Whereas most of these

168 Constitution of Kenya, 2010, article 31(c) and (d).
169 No. 24 of 2019.
170 Data Protection Act, ibid, long title of the Act.
171 Gubbins D, *Digital Credit in Kenya: facts and figures from FinAccess 2019* FSD Kenya (2019) available at https://fsdkenya.org/wp-content/uploads/2020/07/Focus-Note-Digital-Credit-in-Kenya_Updated.pdf last accessed September 26, 2021..
172 Francis E et al., *Digital credit in emerging markets: a snapshot of the current landscape and open research questions'*, Bill and Melinda Gates foundation, 2017, 5.
173 Central Bank of Kenya, *Banking Supervision Annual Report*, 2018.

mobile apps have less than 10,000 downloads, two main apps, Tala and Branch, dominate the market with more than I million downloads each as at 2020. A few more apps had downloads of between 500,000 and I million. Research shows that Tala, Branch, M-Coop Cash, and Eazzy Loan are the most popular mobile lending platforms in the country.[174] The rate at which the apps are uploaded to and pulled down from app stores shows the ease with which the market operates. In addition, the ease with which the download and sign-up is done by customers reflects how easy it is to obtain digital credit in the country, oblivious of the repercussions.

The digital lending apps do not require customers to provide any security to obtain loans, as Shylock asked Antonio to provide in *The Merchant of Venice*. This is meant to lure customers to apply for as much loan as possible, the only requirement being that they must commit to pay back on time. The loan must be paid back between a week and a month, except KCB M-Pesa which allows members to pay back within six months. Interest ranges between 5% and 10% and can sometimes be higher than this. Penalties are levied for failure to pay back on time, and default in payment leads to the defaulter being listed with the Credit Referencing Bureau (CRB), therefore tainting their creditworthiness.

The third model arises when a bank directly offers digital credit to its customers without collaborating with MNOs. For example, Equity Bank operates the Equitel product line which allows customers' unfettered access to their linked Equity bank accounts as well as ordinary mobile network operations (Calls, Text, Internet Data bundles, mobile money transfer, mobile payments etc.).[175]

Some of the digital lenders operate internationally, making it even more difficult to trace their operations, license, and regulate them. For example, Branch International has offices in Mexico, Mumbai, Lagos, San Francisco and Nairobi. They entered the Kenyan market in 2015. The lender provides loans to Kenyan customers ranging from Kshs. 1000/- and Kshs 50,000/-. The loan is repayable in three equal weekly instalments, along with the interest. The interest rate depends on the creditworthiness of the borrower and their commitment to pay the designated weekly instalments.[176] At clause 5 of the Terms and Conditions for acceptance to download and operate the app, the lender states that the customer agrees to authorise the lender to access all personal information related to credit score, date of birth, name, gender, mobile phone number, national identification number, and such other information that will enable the lender to identify the customer. The lender

174 Kaffenberger, Michelle and Edoardo Totolo. 2018. 'A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania''. Working Paper. Washington D.C. CGAP.

175 Mugo M and Kilonzo E, *Community- level impact of financial inclusion in Kenya with particular focus on poverty eradication and employment creation*, Central Bank of Kenya, 2017, 5

176 Drexler, Alejandro and Fischer, Greg and Schoar, Antoinette, 'Keeping it Simple: Financial Literacy and Rules of Thumb', January 2011.

even has authority to access phone data like call history, messages, contacts, and any other crucial data.[177] Data collected from this research shows that some of these digital lenders, including Branch International, sometimes contact the people in the customer's phone book, asking them to remind the customer to repay the loan. This paper will assess whether such acts are in breach of privacy laws.

In what was seen a measure to curb predatory pricing by digital lenders, Google issued user guidelines on several aspects of digital lending in September 2019.[178] Google owns the Google Play Store in which the mobile lending apps are uploaded by digital lenders and then downloaded by customers. Specifically, on personal loans, Google required advertisers of personal loans to provide adequate information regarding the destination site of the creditor. Notably, digital lenders do not disclose their physical location, based on the data collected for this research. The loans are applied on mobile phones and are repaid on the same mobile phones.

Google continues to note that the providers must always indicate the minimum and maximum repayment period when advertising the loans. Secondly, the providers must always indicate the Annual Percentage Rate (APR) which essentially includes interest rate, attendant fees and penalties, and any other costs as allowed by the local law. Thirdly, Google required the providers to always indicate the expected total cost of the loan. This would allow the customer to accept the loan on a point of information. Fourthly, Google indicates that the user guidelines are meant to protect Google customers from harmful and deceptive products, such as high-cost personal loans. Data collected for this research shows that digital lenders do not implement these guidelines as issued by Google. Instead, they indicate the measures taken to implement the guidelines on the app, to deceptively convince Google that the measures are being implemented, yet the measures are not implemented when issuing the loans to customers.

This paper will examine this problem in four themes: permissions granted by customers when installing digital lending apps in their devices, data protection and privacy, consumer protection, and the regulation of digital services as far as lending apps are concerned.

3.0 App Permissions and the Resulting Data Breach

The rapid proliferation of digitally derived data such as social media data, financial transactions data, applications data, and telecommunications data has largely contributed to the rapid expansion of digital credit in Kenya. Digital operators have access to a lot of data from their consumers, especially when they have cookies. In the absence of law and

177 See clause 5.3.3 of the Terms and Conditions, available at https://branch.co.ke/tou, accessed on October 9, 2020.

178 Google, (2019). Financial Products and Services. Available at https://support.google.com/adspolicy/answer/2464998?hl=en, accessed on September 27, 2021.

policy to regulate data access and use, these digital operators can access a lot of consumer data and in the end violate consumer right to privacy and dignity.[179] Most consumers do not know for what reason the digital operators want to use the data, and they easily grant permission for access of their personal data.[180] The digital lending apps are designed to mine as much data as possible to facilitate the determination of the creditworthiness of the customer.[181] For example, the app will access customer data such as contacts, GPS location, call logs, messaging, internet use, previous borrowing trends, and cash flow trends within the device. The digital lending app can only access the data if the customer grants it permission. However, the customer does not have a choice as they will not be allowed to sign up and access credit if they do not grant the app the permissions.[182] Therefore, the customer is placed between a rock and a hard place and forced to choose between Baal and Beelzebub.

Once the apps are downloaded, the customer is required to provide their mobile phone number, full name, national identification number, email address, and such other basic bio data. Some lenders also require the customers to provide data about their income, that is, whether they are employed or not and how much they earn per month. Other lenders require the customers to sign up using their social media accounts like Facebook and Twitter. Every app that was examined in this research required customers to grant access to all phone and social media data. The apps updated their systems to ask for permission from customers to access their phone data when Google updated its user policies. Previously, the apps directly accessed such data without asking for permission from users. In the user policy, Google requires app developers to only use the data for purposes that their customers have consented to.[183] This is difficult to implement, because most customers hardly ever follow up to know how the app developers are using the data that they have permitted them to use.

The apps have terms and conditions which very few customers read before granting permissions. More than 50% of the people interviewed in this study were not aware of the terms and conditions to which they "consented" while granting permissions. The most common clause in the terms and conditions is that the customer will authorise their mobile

179 For an overview of the use of alternative data for financial access, see Elena Mesropyan on the good and bad practices, available at https://gomedici.com/alternative-data-financial-access-good-bad-ugly . Accessed on September 26, 2021.

180 AFI consumer empowerment and market conduct working group, November 2017, "Digitally derived credit: Consumer protection issues and policy responses to new models of digital lending" AFI

181 Insights from a digital lender operating in the Kenyan market revealed that relying on credit scores provided by Safaricom, a mobile network operator with a mobile money product, increased the lenders loan ticket size by up to 250% when compared to using the lender's own data. Available at https://fsdkenya.org/blog/data-sharing-models-the-potential-for-financial-innovation-and-the-risks-that-must-be-managed/ accessed on September 27, 2021.

182 Daryl Collins, Jonathan Morduch, Stuart Rutherford, and Orlanda Ruthven (2010). *Portfolios of the Poor: How the World's Poor Live on $2 a Day.* Princeton University Press.

183 See Google, "Permissions", available at https://support.google.com/googleplay/android-developer/answer/9888170?hl=en. Accessed on September 26, 2021.

service provider (that is, Safaricom, Airtel, Telecom, etc.) to vital information that the app requires. Timiza, for example, requires the customer to consent to authorise Safaricom to share data with the "bank" pursuant to the agreement between the customer and Safaricom. This means that Timiza, the digital lender, is interfering with the agreement that it is not privy to. The digital lender also requires the customer to authorise it to request additional information from Safaricom regarding M-Pesa, M-Pesa system, and Safaricom services as the "bank" will deem fit. For this condition, the customer is not even made aware what kind of additional data the lender will require from Safaricom. The customer therefore proceeds to authorise Safaricom to allow the lender access to all data, as the lender will need from time to time. Branch International clearly states under clause 2.2 of its terms and conditions that the customer will not be allowed to access the system if they click "decline" when the system requires them to either accept or decline.[184]

It is not clear how this conduct by the digital lenders regarding permissions can be regulated under Kenyan Law. The law on this subject is a fragmented one. The starting point is the data Protection Act of 2019.[185] This Act was enacted to give effect to article 31(c) of the Constitution of Kenya which states that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. The Act defines "data" in several ways: information which is processed by means of equipment operating automatically in response to instructions given for that purpose, information which is recorded with intention that it should be processed by means of such equipment, and information which recorded as part of a relevant filing system. A person has a right to be informed of the use to which their personal data is to be put.[186] They also have a right to object to the processing of all or part of their personal data.[187] This is not possible for customers of digital lending apps because if they object to the processing of all or part of their data then they will not obtain the credit they are looking for.

When the data is being collected, a person has a right to be informed of the data that is being collected, the fact that personal data is being collected, the third parties to whom the data will be transferred to, and a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data.[188] Mobile digital lenders do not do this. In fact, once they have been granted permission to mine data from the customer's mobile device that is the last time the customer will be informed about their data. This is in breach of the customer's rights under the Constitution and the Data Protection Act.

184 See clause 2.2 of the "Terms of Use", available at https://branch.co.ke/tou, accessed on September 25, 2021
185 The Data Protection Act, No. 24 of 2019.
186 Section 26(1).
187 Section 26(3).
188 Section 29(a), (b), (c), and (f).

Section 72 of the Act creates several offences arising from breach of data protection law. For example, it is an offence for someone to use personal data in any manner that is incompatible with the purpose for which such data has been collected, without any lawful excuse.[189] It is also an offence to access personal data from a person who controls that data without their permission.[190] Disclosing personal data to a third party is also an offence.[191] For these offences, the Act creates a penalty of a maximum fine of three million shillings or a maximum of ten years in jail. In addition to the fine or jail sentence, a court may order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence,[192] or order or prohibit the doing of any act to stop a continuing contravention.[193]

Mobile digital lenders in Kenya violate this law all the time. First, they access data that they have not been authorised to access, sometimes because of the naivety of the customer. Secondly, they share this data with third parties like telecommunication companies and persons in the contact list of the customer's device. It is not easy to charge them with the offences under the Data Protection Act because some of them are unregulated. There are those lenders that upload their apps on app stores and pull them down as they wish. There is therefore need for further review of applicable law, because the consumer may have their rights violated, yet the culprits are not charged with the listed offences under the Act.

The Kenya Information and Communications Act of 2012,[194] was enacted to, among other things, facilitate the development of the information and communications sector. The most relevant Part is Part VIA titled "Electronic Transactions." The Act empowers the Communications Authority of Kenya to facilitate electronic transactions by ensuring the use of reliable electronic records.[195] It also empowers the Authority to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.[196] The Act further requires the Authority to develop sound frameworks to minimize the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions.[197] Part VIA of the Act therefore positions the Communications Authority of Kenya as the custodian of all electronic transactions in Kenya, so that if certain electronic transactions violate the Act, the Authority has powers to act against the persons or entities carrying out such violations. Digital creditors operate apps that are designed, uploaded, and

189 Section 72(1).
190 Section 72(3)(a).
191 Section 72(3)(b).
192 Section 73(2)(a).
193 Section 73(2)(b).
194 Cap 411A Laws of Kenya.
195 Section 83C(a).
196 Section 83C(d).
197 Section 83C(f).

downloaded through electronic devices. Therefore, the Authority has powers under part VIA of the Act to regulate their operations.

The Act also empowers the Authority to license all entities that operate electronic certification system, repository or a sub-domain in the Kenya country top level domain (.ke ccTLD).[198] If a person contravenes the provisions of the Act in this Part, they commit an offence and are liable on conviction to a maximum fine of three hundred thousand shillings or to a maximum prison sentence of three years, or both. Ordinarily, lending in Kenya is regulated by the Central Bank of Kenya, as the Central Bank is the institution that regulates the banking industry in the country.[199] However, as it will be demonstrated later in this paper, digital lenders are not deposit taking institutions and therefore they are not banks. The Central Bank of Kenya regulates banks; banks are deposit taking institutions. Most of the current digital lenders in the country are unlicensed, and this may explain why they are often pulled out of app stores and replaced.

4.0 Data Protection, Privacy and Customer Consent

Digital operators usually require their customers to consent to access to data stored in their digital spaces and other spaces that the digital operator may want to access. The presumption is that when someone ticks "yes, I agree" to a box requiring them to accept the terms and conditions, they have read and understood those terms. Murphy and Medine (2018) write that consent is not enough in data access.[200] This is because people rarely read online contracts and oftentimes accept the terms and conditions without ever reading them. A recent study by Deloitte showed that 91% of the 2000 respondents who were interviewed accept terms and conditions without ever reading them.[201] Their findings are backed by further empirical evidence. For example, Obar and Oeldorf-Hirsch carried out an experimental survey with 543 respondents to establish to what extent people ignored privacy policy and terms of service on the internet.[202] They designed a fictitious internet site, NameDrop, and created a fictitious privacy policy and terms of service. They then required users to "accept" those terms before accessing the site. Results showed that 74% of the respondents ignored the requirement and proceeded to quickly accept the terms without attempting to read them.

198 Section 83D(1)(a) and (b).

199 See section 4Z of the Central Bank of Kenya Act, Cap 491 Laws of Kenya.

200 Gayatri Murthy, and David Medine (2018). "Data Protection and Financial Inclusion: Why Consent Is Not Enough". Available at https://www.cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough. Accessed on October September 27, 2021.

201 Caroline Cakebread (2017). "You're not alone, no one reads terms of service agreements", available at https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?IR=T, accessed on September 27, 2021.

202 See Obar, Jonathan A. and Oeldorf-Hirsch, Anne, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (June 1, 2018). Information, Communication & Society, pp. 1-20, 2018., TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016., Available at SSRN: https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465, accessed on September 27, 2021.

Even if users were to be careful and decide to read the privacy policies and terms of service, research shows that it would take them very long to complete reading them. Cranor and McDonald (2008) carried out an experiment to calculate the time it would take users to read all the privacy policies that they are required to read. The authors found that the average length of the privacy policy and terms of service for the top 75 websites that they used as case studies was 2,514 words. Assuming that the average reading rate in academic literature was 250 words a minute, they estimated that a person would take 10 minutes to read one privacy policy in the websites. They also estimated the average number of websites a person visits per year and found that 1,462 websites were visited. From their calculations, a person would therefore spend 25 days from their calendar year reading privacy policies. Using economic regression formulae, they further estimated that the opportunity cost for reading the privacy policies would be $781 billion for the entire US.[203] This means that reading those privacy policies, though to the benefit of the user, requires the user to incur huge opportunity cost.

The privacy policies and terms of service exist to enable companies owning the websites to avoid legal trouble, as there will be evidence that the customer accepted the terms. However, customers do not have a choice, because they are not allowed to access the site if they do not accept those terms. The consent requirement therefore plays no role in enhancing credibility and ensuring that the dignity of the user is upheld.[204] Privacy policies and terms of service are long and are drafted by the company's legal teams to reduce the company's liability as much as possible in the event of loss to the customer. They are also meant to grant the company close to free reign over the customers personal data. These digital apps have been found to track every move that the user makes and can then report back to the designers.[205]

This study reviewed the privacy policies of leading digital lenders under four key heads: Whether the lender has a clause on its terms and conditions committing itself to respect user's dignity and privacy, whether the lender commits to using the data only for business purpose, whether the lender shares the data to third parties and whether they seek consent from the user before sharing such data, and whether the user has any rights in the use of their data by the lender. Results show that a total of 14 of the apps reviewed in this study have data privacy policy that is distinct from the terms and conditions. Shockingly, though, six of these lenders have similar privacy policies. There is every reason to believe

203 Lorrie Faith Cranor and Aleecia McDonald (2008). "The Cost of Reading Privacy Policies". Journal of Law and Policy for the Information Society, Volume 4:3, Pp 543-568.

204 See Rahul Matthan (2018). "Do away with consent to strengthen data privacy", available at https://www.livemint.com/Opinion/ksxauMlxKS8UsuScPs114K/Do-away-with-consent-to-strengthen-data-privacy.html, accessed on September 27, 2021.

205 See Jennifer Valentino DeVries, Natasha Singer, Michael Heller, and Aaron Klorik (2018). "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret". Available at https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?action=click&module=Top%20Stories&pgtype=Homepage, accessed on September 27, 2021.

that either all the six lenders copied from the same source or five of them copied from one of the lenders. Results also show that all the lenders that were reviewed in the study share customer data with third parties without seeking the consent of the customer. Data is shared with Credit Reference Bureaus (CRBs) while mobile service providers provide access to customer data that they hold in their servers. Some lenders even contact the customer's contacts in the phone book, asking them to request the customer to pay the loan that is due, when the customer defaults in payment. Other lenders have clauses that allow it to decide how to use the customer data without seeking the customer's consent. mKey, a digital lender, for example has a clause giving it the sole discretion of deciding what to do with the data. Tala, another digital lender, stores the data and uses it even after the customer has stopped using the app and deleted it. The lender requires the customer to waive their rights over the data by accepting the terms and conditions.[206]

The right to data privacy is anchored by the Constitution. Every person has a right to data privacy, which includes not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed.[207] When lenders share their customer data to third parties and ask third parties to help them access customer data, they breach the customer's right to data privacy which is anchored in the constitution. This breach of the salient constitutional right to data privacy mostly escapes unchecked because of the largely unregulated nature of the industry. For example, the lenders who have violated this right and have already discontinued their operations by pulling their apps from the app stores have effectively escaped sanctions. Their customers' data therefore remains in the virtual spaces and can be misused for a long time.

5.0 Some Legal Frameworks on Data Protection

The Data Protection Act was sponsored and introduced in the National Assembly by the Leader of Majority Party in the House on July 4, 2019 and assented to on November 8, 2019. The legislative process only took 4 months. The object and purpose of the Act is stated at section 3 as "(a) to regulate the processing of personal data; (b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25; (c) to protect the privacy of individuals; (d) to establish the legal and institutional mechanism to protect personal data; and (e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act."[208] When the bill was being debated in the National Assembly, Members were categorical that it was the privacy of individuals that the bill would protect. Honourable Millie Odhiambo-Mabona (MP Suba North) stated as follows:

206 https://tala.co.ke/privacy-policy-ke/, accessed on September 27, 2021.
207 Constitution of Kenya, 2010, article 31(c) and (d).
208 Section 3, Data Protection Act

> *"I am seeking to amend Clause 3 of the Bill by inserting a new paragraph after paragraph (b) to include - "to protect the privacy of individuals" The main purpose of this Bill is to protect the privacy of individuals and yet in the objectives, we have not provided for that. So, I am only just stating that we are protecting the privacy of individuals"*[209]

Section 8(2) provides that the Office of the Data Commissioner which is established at Part II of the Act may collaborate with national security organs. When MPs were debating this bill, Honourable William Kisang (MP, Marakwet West) stated as follows:

> *"You know we have our data now, say, Huduma data, IDs or intelligence data. So, basically, they should work together. I believe when the National Security Council meets, this officer should be there. They also need to inform security agents what is happening. They will be holding serious and important data for the citizens of this country*."[210]

Clearly, the National Assembly was not enacting a law to regulate the misuse of data by digital actors like digital lenders. They had a different kind of purpose in their minds. The enactment of this law was triggered by the decision of government to introduce a central depository system for several aspects of personal data. The system was an initiative of the Government of Kenya and was referred to as the National Integrated Identity Management System (NIIMS) program, initiated through Executive Order No. 1 (2018). The government's idea was to "create and manage a central master population database which will be the 'single source of truth' on a person's identity. The database would contain information of all Kenyan citizens and foreign nationals residing in Kenya and will serve as a reference point for ease of service delivery to the people of Kenya."[211]

Section 19 of the Act requires data controllers and processors to apply to the Data Commissioner for registration and that Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration. The way some digital lenders operate in Kenya does not give room for such application. As noted earlier, some digital lenders are app-based and the proprietors simply design and upload them on app stores for their customers to download. They do not have a reason to seek registration by the Data Commissioner. Honourable William Kisang stated as follows regarding the need for renewable of the registration certificate by data processors, a statement which supports the argument in this paper that some data processors do not require registration:

> *"Hon. Temporary Deputy Chairlady, I support Hon. Duale's amendment. We agreed that there are those data processors and data controllers who do not have to get licences. Say, when you go to*

209 National Assembly Debates, November 6, 2019. Parliament Hansard. Available at http://www.parliament.go.ke/sites/default/files/2019-11/Hansard%20Report%20-%20Wednesday%2C%206th%20November%202019%28P%29.pdf, accessed on September 22, 2021

210 Ibid, at page 28.

211 Republic of Kenya, "Huduma Namba", Available at https://www.hudumanamba.go.ke/, accessed on September 22, 2021

> *any office, there are security officers who take your details like your ID number or telephone number and then you are allowed in. Such data processors and data controllers do not need to get licences. So, that is why the discretion is there, to weigh in. I believe the person who will be appointed as a Data Commissioner will be a reasonable person who has gone to school properly".*[212]

The principles and obligations of personal data protection are provided in section 25 of the Act. One of the principles and obligations is that data processors and controllers shall ensure that personal data is not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject. Digital lenders operate through the internet and the internet has no territorial boundaries. This is a principle that controllers and processors of digital borrowers' data cannot abide by. Honourable Godfrey Osotsi (Nominated MP, ANC Party) recognised this fact during the debates in the National Assembly when he stated as follows:

> *"I think we need to be very careful with these issues of data processing. Consent is already implied. If you look at the obligations of a data processor and data controller, we may not be able to process data if we put that amendment here, from a technology point of view. We have so many banks and insurance companies like Safaricom who have data centres outside the country. We will not be able to process any data if we put so much restriction on data processing. Obligations of data processors and data controllers are already implied".*[213]

Furthermore in 2019, the Central Bank of Kenya received a parliamentary resolution requesting the regulator to develop regulatory guidelines for digital lenders and in the same year, nominated Member of Parliament sponsored The Central Bank of Kenya (Amendment) Bill, 2020 in the National Assembly. The Bill was later passed into law in 2020. The Act amends the Central Bank of Kenya Act of 2014 as section 4A to empower the Central Bank of Kenya to regulate and supervise the conduct of providers of digital financial products and services.[214] It also empowers the Bank to regulate and supervise the conduct of digital credit providers and digital credit service providers.

The Central Bank of Kenya is therefore now empowered to regulate digital lenders in the country through this law. However, several questions remain unanswered. For example, will the Bank also license new digital lenders intending to join the industry? Will the Bank collaborate with App Stores to ensure that lenders that are not licensed are not accommodated in the App Stores? Will the Bank carry out a post-mortem of the existing digital lenders that are currently operating in the country to ensure that they are licensed and operate within the confines of the law? The way app-based digital lenders operate make it difficult for the CBK to trace and regulate them unless it is adequately resourced.

212 National Assembly Debates, note 49 at page 35
213 Ibid, at page 38
214 Section 2 of the Central Bank of Kenya (Amendment) Bill, 2020.

6.0 Conclusion

Through the Central Bank of Kenya (Amendment) Bill, 2020, the Central Bank of Kenya has been empowered to regulate the digital lending industry. The Act amends section 4A of the Central Bank of Kenya Act by inserting new paragraphs to empower the Bank to regulate digital financial products in the country.

However, the nature of this industry means that the Bank is not adequately empowered to regulate it. It is conceded that the Bank can indeed regulate digital financial products that are sold by mainstream banks in the country, for example, Equity Bank's Eazzy Loan app, Kenya Commercial Bank's KCB M-Pesa, and Commercial Bank of Africa's M-Shwari. However, it is a huge challenge for the Bank to regulate unlicensed digital financial products that are currently operating in the country. These lenders upload their apps on App Stores and pull them down at will. They are still able to conduct their business in the country even without being licensed by the Bank.

Whereas the Bank can regulate the finance aspect of the business, several aspects remain unregulated, for example, licensing, app permissions, data protection, privacy, dignity, consumer protection, and pricing of loans. The Data Protection Act is also not a comprehensive legislation, as it did not anticipate the kind of business digital lenders operate and the kind of data they collect. One way of enhancing data protection in the country is by empowering and adequately resourcing the Communications Authority to have capacity and competence to trace, license and regulate digital lenders as they operate digitally. The Communications Authority has mandate to enforce the Kenya Information and Communications Act which is the legislation that regulates all forms of electronic communication.

Another way of ensuring that customer data is well protected is by empowering the Office of the Data Commissioner to trace, register and regulate all app-based digital lenders in the country, both the licensed and the unlicensed ones. This office can discharge its mandate by collaborating with App Stores like Google Play Store. The CBK can regulate the finance aspect of the lenders, but it does not have capacity to regulate the digital aspect.