2024 IEEE International Symposium on Technology and Society (ISTAS) | 979-8-3315-4070-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISTAS61960.2024.10732051

A License to Prey: Investigating the Impact of Digital Loan App Regulations on Permission Requests and Privacy Policies in the Kenyan Market

Alexis Morales Flores, Michael He, William Wu, Imani N. S. Munyaka
Computer Science and Engineering
University of California San Diego
La Jolla, USA
amoralesflores, mih024, wiw010, drmunyaka@ucsd.edu

***Abstract*—The availability of mobile money in Kenya has positively impacted commerce, financial transaction efforts, and the ability of individuals to receive and save their money. The addition of mobile loan applications provides access to loans without the hassle of going to a physical bank and, in some cases, completing paperwork. While it has its benefits, limited protection of user data has been a cause for concern. User complaints prompted a change in the mobile loan industry, requiring applications to be licensed and banning the use of specific permissions for Android versions of the apps placed in the Google Play Store. We investigate the impact of this change and explore ways to improve regulation by reviewing 30 licensed (n=15) and unlicensed (n=15) Kenyan-targeted digital lender apps. The results suggest that regulation has not yet had a significant impact on digital lender app development and thus encourages government-supported development guidelines and audits.**

Keywords— digital loans, privacy, permissions, Android

I. Introduction

In the global south, digital banking offerings have increased consumer access to money in times of need. Using digital banking, citizens no longer have to worry about exchanging currency and the need to carry physical money or cards. Digital banks provide benefits such as the ability to spend and save money without living close to a physical branch, opening an account without being near a bank, and cash-less transactions, among other innovations [1]. In Kenya, many citizens use M-Pesa, a popular mobile money product [2] developed by Safaricom Company Ltd, a network operator in the country. M-Pesa provides a financial transaction service that works with and in parallel to traditional banking systems [3]. Customers must first register to use the service, which can be done at various authorized agents which often includes retail shops not directly associated with Safaricom, like a food market. At these locations, customers can then deposit money in exchange for electronic money in their accounts. The ease of access has led to 50 million active M-Pesa users in Africa as of 2021 [4]. Prior work also suggests that the adoption of M-Pesa has provided some women with a safe place to store their money, reduced or removed the costs related to financial services, improved the efficiency of business tasks, and increased access to social capital [5]–[7].

However, although there has been an increase in digital transactions [8] and use, the move to digital banking requires that applications be safe and secure to protect user privacy. Consumers and researchers alike have identified security and privacy concerns related to using M-Pesa and other financial mobile applications [9], [10]. In particular, Munyendo et. al published a paper in 2022 exploring the concerns of mobile loan app users in Kenya [11]. Their work highlighted user concerns which include privacy concerns related to permissions requested and data sharing with third parties. This is not surprising since, in 2020, consumers borrowing money from OPesa and OKash (Chinese-owned companies) were warned about continuing the use of those applications due to reports claiming that OPesa and OKash applications would publicly shame users who owed money by reaching out to people on their contact lists to recover money owed [12].

To protect users, the Kenyan government released the Data Protection Act in 2019 [13], required digital credit lenders to acquire a license to operate starting in 2022 [14] and allowed the lender regulator Central Bank of Kenya to increase the number of steps mobile lenders must take before they can add users to Kenya's Credit Records Bureau Credit Information Sharing System. These changes coincided with Google's ban of personal loan apps that were not licensed by the Central Bank of Kenya [15] and its policy update that prohibited the use of specific permissions by personal loan apps [16].

These previously identified problems and new solutions have led us to identify the lessons other countries learn from the digital lending case in Kenya. To do this, we collect and analyze a total of 15 licensed and 15 unlicensed mobile loan applications targeted toward the citizens of Kenya. Through our analysis, we aim to answer the following research questions:

1) **How does Google's permission ban influence the permissions used by apps?**
2) **How do Google's permission ban and the**

Kenyan government license requirement influence privacy policy content?

We collect the two versions of each app (before and after the licensing law), thus analyzing 60 apks. Each application was evaluated using MobSF and Jadx to identify permissions requests to directly evaluate the impact of Google policy changes and Kenyan Law. We make the following contributions:

1) To our knowledge, we are the first to compare app permissions of Kenyan-targeted digital loan applications before and after a change in Kenyan law and Google terms of service.
2) We identify personal credit lending apps in the Google Play store that do not meet the terms of service.
3) We provide support for additional consequences, regulations, and oversight of personal credit lending applications that are added to the Google Play store.

II. Methods

We gathered 30 pairs of mobile loan applications in Kenya for our study to identify the changes (if any) in permission requests. Each pair consisted of a version prior to the Central Bank of Kenya's Digital Credit Providers Regulation, and another following its enactment. We divided our apps into two distinct categories: 15 app pairs were licensed by the Central Bank of Kenya, while the other 15 were unlicensed. Android versions of the digital lender applications were collected from Android Package Kit (APK) repositories APKpure, APK Mirror, and APK Combo, which have been used in prior work [17]–[19]. We collected the earliest versions of each app that was available before March 18th, 2022 when the regulatory measure went into effect and the latest version of the app available in January 2024. Mobile Security Framework (MobSF) is an automated framework that analyzes Android and iOS mobile applications for security and privacy vulnerabilities [20]. We used this tool to analyze each app and for the purpose of this short paper, we report the permission request results only. We review 30 apps due to the consistent removal of unlicensed apps in the Play Store, and short (n=15/32) list of licensed digital credit lenders with apps in the Play Store.

A. Permission Requests Analysis

For permission analysis, we focused on the six permissions prohibited by the Google Play store [] but located in the 'AndroidManifest.xml' file for the app. Each of these permissions can be abused to gather personal information about the consumer. (1) READ_EXTERNAL_STORAGE allows the app to access files stored on external drives, such as SD cards, which may contain personal user files. (2) READ_CONTACTS would allow the app to view the user's contacts list, while (3) READ_PHONE_NUMBERS would authorize the app's read access to the device's phone numbers. Furthermore, (4) ACCESS_FINE_LOCATION gives the app permission to access fine location resources such as the global positioning system (GPS) to identify the precise location of the user's device at any given time. (5) READ_MEDIA_IMAGES allows an app to read image files from external storage. Lastly, (6) WRITE_EXTERNAL_STORAGE allows an application to write to the device's external storage.

B. Privacy Policy Analysis

We collected the privacy policy link for all the apps reviewed. We used the privacy policy linked on the app page of the Play Store. We searched each privacy policy for keywords related to the prohibited permission requested. We searched for the following keywords: external storage, media, images, photos, contacts, and phone numbers. If the privacy policy discussed collecting this information at any length and depth, we counted that as a discussion of the permission in the privacy policy.

TABLE I
App Permissions Before and After March 23rd, 2023

Licensed Apps	Before	After
Equity Mobile	📞🌍📦✏️	🌍📞📦✏️
HF Whizz	🌍📞✏️	🌍📞✏️
HFC Whizz	🌍📞✏️	🌍📞✏️
iPesa	🌍📞📦✏️	-
KCB*	🌍📞✏️	🌍📞✏️
KWFT Mobile*	🌍📞📦✏️	🌍📞
M-KOPA	-	-
M-PESA*	🌍📞📦✏️	🌍📞📦🧑🏾✏️
MySafaricom*	📞📦✏️	🌍📞📦✏️
Pezesha Marketplace	📦✏️	🌍📦✏️
TALA	🌍📞📦✏️	🌍📞📦✏️
Timiza*	📞📦✏️	📞📦📷✏️
VOOMA*	🌍📞📦✏️	🌍📞📦✏️
ZASH LOAN	🌍📞📦🧑🏾✏️	-
Zenka Loan Kenya	🌍📦✏️	-
Unlicensed Apps	**Before**	**After**
Berry	🌍📞📦✏️	🌍📦
Branch	🌍📞📦✏️	🌍📦📷
Brigit	🌍📦✏️	-
CashNow	🌍📞📦🧑🏾✏️	🌍📞📦🧑🏾✏️
DirectCash	-	-
Kiva	🌍📞📦✏️	-
MoneyLion	🌍📞📦✏️	🌍📞📦📷✏️
Numida	🌍📞📦✏️	🌍📞📦📷✏️
OKash	🌍📞📦✏️	🌍📞📦✏️
OneMain	-	-
OPesa	🌍✏️	🌍📞✏️
Possible	📦✏️	📦✏️
Utunzi	-	🌍📞✏️
Zidisha	🌍📞📦✏️	🌍📞📦✏️
Zuri Cash	🌍📞📦✏️	-

📞 = Read Contacts, 🌍 = Access Fine Location,
📦 = Read External Storage, 🧑🏾 = Read Phone Numbers
✏️ = Write External Storage, 📷 = Read Media Images
* Banks

III. Results: Use of Banned Permissions

We used the scipy.stats package in Python to conduct a Chi-Square test of independence [21]. This test was used to determine if the number of apps that requested specific permission significantly changed once digital lending apps were required to be licensed.

A. Licensed Apps

For app permissions, we compared old and new versions of licensed apps and found that reading external storage saw a reduction of 26.66% whereas 11 apps (73.33%) requested these permissions before regulation but only 7 apps (46.67%) requested it after regulation. Reading contacts also decreased by 13.33% from 12 apps (80%) to 10 apps (66.67%), while requests to access fine location and read phone numbers remained consistent with 10 apps (66.67%) and 1 app (6.67%), respectively. The request for reading media images increased from 0% to 6.67% (1 app) while write external storage decreased from 93.33% on 14 apps to 66.67% to 10 apps.

B. Unlicensed Apps

Permissions for unlicensed apps indicate that requests for reading external storage experienced a decrease of 20%, with 11 apps (73.33%) seeking this permission pre-regulation, as opposed to 8 apps (53.33%) post-regulation. Similarly, the solicitation for reading contacts exhibited a 13.33% reduction, transitioning from 9 apps (60%) to 7 apps (46.67%). Accessing fine location also saw a reduction of 13.33% from 11 apps (73.33%) to just 9 (60%), while writing to external storage also decreased by 26.67% from 12 apps (80%) to only 8 (53.33%). Conversely, requests to read phone numbers remained consistent, with only a single app (6.67%) requesting the same permission before and after the licensing law. Notably, reading media images increased from 0% to 20% which was found on 3 applications.

Our analysis did not reveal any significant changes in the number of banned permission requests after performing a Chi squared test for independence.

C. Unlicensed & Licensed Apps.

Before 2024, at least 21 of the apps we reviewed had access to user contacts, 22 could read and 26 could write to external storage respectively, 21 had access to the fine location, 2 were able to read phone numbers, and none of them asked to read images or videos. As of May 23, 2023, 17 of the apps requested access to user contacts, 18 to write external storage, 15 to read external storage, 19 to fine location, 2 asked to read phone numbers, while 4 had requested access to images, or videos.

D. Privacy Policy

After reviewing app permissions, we evaluated each app's privacy policy to see if, at minimum, the document explains the type of data it is requesting to collect. The results show that 26% or 5 apps out of 19 apps discussed accessing the location from the app. 25% or 5 apps out of 20 discussed collecting the phone numbers or contacts from users. None of the apps that request reading external storage mention reading or writing to storage in their privacy policy. The majority of the apps (84%, 16 apps out of 19) that requested to read media and images discussed collecting media and images from the user's device.

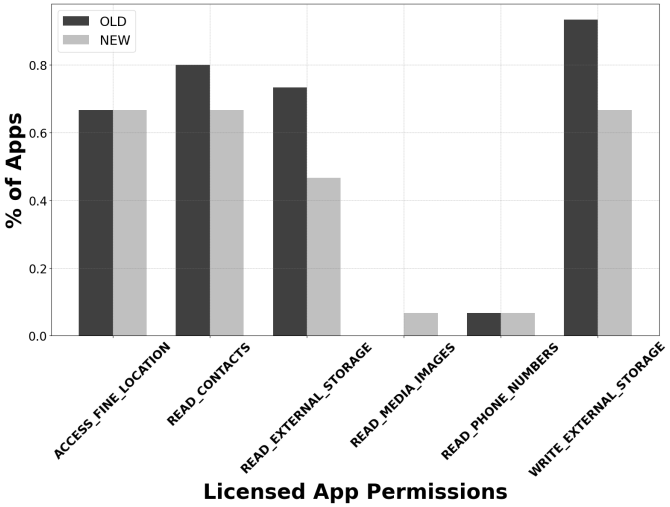

Fig. 1. Permissions Requested by Licensed Apps

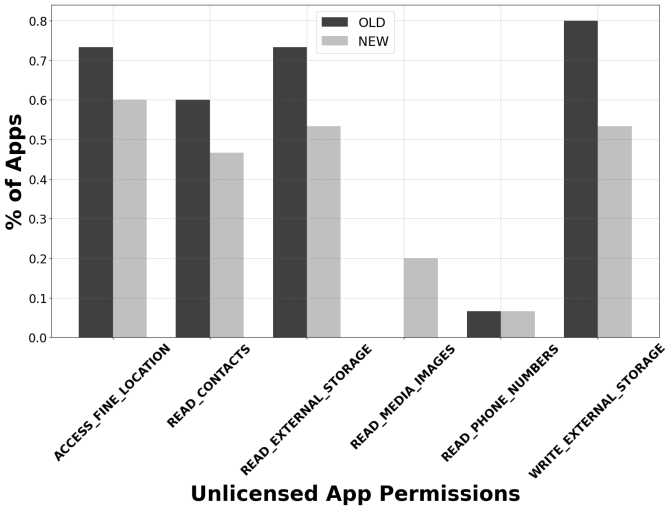

Fig. 2. Permissions Requested by Unlicensed Apps

IV. Ethical Considerations

We will alert the Google Play Store about these applications before this paper is published. We are happy to note that OPesa has been removed from the Play Store during the time of the study.

V. Discussion

In this section, we answer the three research questions presented in the introduction. Additionally, we provide

recommendations for various shareholders in the digital lending ecosystem.

A. What impact does having a permission ban have on the apps permission requests?

Since the change in permission use is small, we believe it showcases the limited power of regulation in the mobile loan application industry for all applications. Furthermore, it also suggests that Kenya's licensing regulations may not meaningfully impact the amount of permissions requested by mobile credit lenders. Branch, an unlicensed app, changed its permission requests over time. Tala and Zenka received their license in March 2023. Additionally, Opesa, an app notable for its bad practices, has also removed such permissions as of 2021.

However, these small changes do not change the fact that personal loan applications are banned from using these permissions in the Google Play Store. Thus, we encourage Google to automatically check for the use of these permissions when credit lending apps are added to the Play Store. Additionally, we also want to highlight that there are limits to prohibiting the use or permissions since there is more than one way for an app to collect personal information. For example, research indicates that Wi-Fi and other cellular signals can achieve approximate location tracking while reducing the need for precise GPS location data collection [22]. Future research might explore how to detect this type of unauthorized use of legitimately requested data.

B. What impact does requesting a banned permission have on the privacy policy?

The difference between the number of apps requesting permissions and mentioning them in their privacy policy is small in some cases. This would suggest that the permission ban may not necessarily impact the way privacy policies are written. Our results do not support the idea that prohibited permission use is hidden or not included in the privacy statements.

C. Suggestions

Easily Accessible & Accurate Information: During our search for each APK collected, we often came across lists of the top applications for personal loans that included unlicensed apps in the recommended lists, many of which are now updated [23]. However, there remains an opportunity for the Central Bank of Kenya to provide recommendations for lenders on how they should operate while waiting for licensing. While they may not be able to stop new digital lenders from operating, they may be able to provide advice to prevent end users from downloading malware or unlicensed apps. For example, the regulator could provide a list of tools that applicants should run their app through to detect security issues or require that unlicensed apps explicitly state their license status in their app. This is also an opportunity for the Digital Financial Services Association of Kenya to provide documentation to assist their community members. They could provide documentation detailing which members have a license to operate and who is still waiting.

Privacy Policy Should Match Requests: Since many of the privacy policies explicitly state that they are collecting the data they have requested access to, we suggest that all companies ensure there is a match between what is requested and what is written in the policy. Prior work has shown that Android app permission requests may not match what their privacy policy [24], [25]

Individualized Privacy Policy Support: Additionally, we suggest that digital lender associations such as the Digital Financial Services Association of Kenya (DFSAK) provide guidelines on which app permissions lenders should request when certain tasks need to be completed and emphasize the importance of discussing data collection in the privacy policy. For example, even though iPesa eventually removed the request to read contacts, they stated the following in their privacy policy:

> "Upon your explicit authorization for uploading call logs, we will reach out to you via a voice call and gather data such as call timestamps, phone numbers, and caller names. This is crucial for confirming the authenticity of the device you are using for our services."

However, reading the contacts from a device is not necessarily needed to authenticate a device [26]. Other apps like Tala and Zash, which request to read contacts, provide multiple reasons as to why they collect information in general but do not explain specifically why they need the list of contacts from their customers' devices. Prior work suggests that providing explanations can increase user trust and privacy awarness [27], thus benefiting both shareholders in the ecosystem.

VI. Conclusion

Our assessment of mobile loan applications in Kenya after the implementation of the Central Bank of Kenya's Digital Credit Providers Regulations of 2022 and Google terms of service update in 2023, provides insight into the regulatory impact on app security and privacy via permission requests. The results suggest that these regulations may not have a significant impact on the information digital lenders collect and how they collect them. However, we suggest that formal consequences, auditing, and development guidelines from all regulating bodies might provide an improvement.The persistence of some privacy risks underscores the need for ongoing regulatory attention and more comprehensive policies.

Acknowledgment

Thank you Anish Devineni, Bryce Ong, Jay Jhaveri, Latanya Khissy, and Sean Pinto, for your support during the app analysis process.

References

[1] P. Kutty. (2018) How is digital banking faring a year after demonetization. [Online]. Available: https://www.entrepreneur.com/article/307472

[2] W. Jack and T. Suri, "Mobile money: The economics of m-pesa," National Bureau of Economic Research, Tech. Rep., 2011.

[3] Vodafone Group, "What is m-pesa?" May 2023. [Online]. Available: https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa

[4] V. Oluwole, "M-pesa africa active users reach 50 million in 2021," *Business Insider Africa*, 2021.

[5] R. M. Gikunda, G. O. Abura, and S. G. Njeru, "Socio-economic effects of mpesa adoption on the livelihoods of people in bureti sub county, kenya," *International Journal of Academic Research in Business and Social Sciences*, vol. 4, no. 12, p. 348, 2014.

[6] E. R. Chebet, "The impact of mobile payments on the performance of micro-businesses: a case of safaricom's lipa na mpesa services in machakos town, kenya," Ph.D. dissertation, University of Nairobi, 2017.

[7] D. White, "The social and economic impact of mpesa on the lives of women in the fishing industry on lake victoria," 2012.

[8] M. Joshi, "Digital payment system: A feat forward of india," in *Research Dimension*, 2017.

[9] C. N. Thuo, "Influence of mpesa cashless payments product on the operations of east africa breweries distributors in nairobi county," Ph.D. dissertation, University of Nairobi, 2014.

[10] R. Nyakemwa, "Impact of mobile banking risks on financial inclusiveness: an mpesa study," Ph.D. dissertation, The University of Nairobi, 2012.

[11] C. W. Munyendo, Y. Acar, and A. J. Aviv, ""desperate times call for desperate measures": User concerns with mobile loan apps in kenya," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 2304–2319.

[12] J. Owino, "Borrow from opesa and okash at your own risk-dlak," *Business Insider Africa*, 2020.

[13] The Parliament of Kenya, "The data protection act, no.24 of 2019," 2019.

[14] Government of Kenya, "Central Bank of Kenya (Amendment) Act, 2021," 2021, accessed: 2024-06-06. [Online]. Available: https://www.centralbank.go.ke/uploads/acts/2012148989_Central%20Bank%20of%20Kenya%20(Amendment)%20Act,%202021.pdf

[15] A. Njanja, "Google removes hundreds of kenya-focused loan apps from play store," *TechCrunch*, 2023, accessed: 2024-06-06. [Online]. Available: https://techcrunch.com/2023/03/24/google-removes-hundreds-of-kenya-focused-loan-apps-from-play-store/

[16] M. Marcelline, "Google to ban financial lending apps from accessing user photos, contacts," *PCMag*, 2023, accessed: 2024-06-06. [Online]. Available: https://www.pcmag.com/news/google-to-ban-financial-lending-apps-from-accessing-user-photos-contacts

[17] L. Ardito, R. Coppola, S. Leonardi, M. Morisio, and U. Buy, "Automated test selection for android apps based on apk and activity classification," *IEEE Access*, vol. 8, pp. 187 648–187 670, 2020.

[18] K. A. El-Dahshan, E. K. Elsayed, and N. E. Ghannam, "Comparative study for detecting mobile application's anti-patterns," in *Proceedings of the 8th International Conference on Software and Information Engineering*, 2019, pp. 1–8.

[19] N. Nasir, F. Iqbal, M. Zaheer, M. Shahjahan, and M. Javed, "Lures for money: A first look into youtube videos promoting money-making apps," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 1195–1206.

[20] A. Abraham, D. Schlecht, M. Dobrushin, and V. Nadal, "Mobile security framework (mobsf). 2016," *URL https://github.com/MobSF/Mobile-Security-Framework-MobSF*, 2022.

[21] P. Virtanen, R. Gommers, T. E. Oliphant, M. Haberland, T. Reddy, D. Cournapeau, E. Burovski, P. Peterson, W. Weckesser, J. Bright, S. J. van der Walt, M. Brett, J. Wilson, K. J. Millman, N. Mayorov, A. R. J. Nelson, E. Jones, R. Kern, E. Larson, C. J. Carey, İ. Polat, Y. Feng, E. W. Moore, J. VanderPlas, D. Laxalde, J. Perktold, R. Cimrman, I. Henriksen, E. A. Quintero, C. R. Harris, A. M. Archibald, A. H. Ribeiro, F. Pedregosa, P. van Mulbregt, and SciPy 1.0 Contributors, "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python," *Nature Methods*, vol. 17, pp. 261–272, 2020.

[22] F. Li, X. Wang, B. Niu, H. Li, C. Li, and L. Chen, "Exploiting location-related behaviors without the gps data on smartphones," *Information sciences*, 2020. [Online]. Available: https://doi.org/10.1016/j.ins.2019.05.052

[23] G. Mokeira Obiero, S. Ayub, and P. Walubengo, "Loan apps in kenya for genuine instant loans," 2018, accessed: 2024-06-06. [Online]. Available: https://www.tuko.co.ke/281951-loan-apps-kenya-genuine-instant-loans.html

[24] L. Yu, X. Luo, J. Chen, H. Zhou, T. Zhang, H. Chang, and H. K. N. Leung, "Ppchecker: Towards accessing the trustworthiness of android apps' privacy policies," *IEEE Transactions on Software Engineering*, vol. 47, no. 2, pp. 221–242, 2021.

[25] L. Gibert *et al.*, "On the (un)reliability of privacy policies in android apps," *arXiv*, 2023, accessed: 2024-06-06. [Online]. Available: https://arxiv.org/abs/2004.08559

[26] M. Kathiravan, M. Sambath, B. Bhuvaneshwari, S. Nithya Krishna, W. Jeshwin, and N. Babu, "Improved security on mobile payments using imei verification," in *Sentiment Analysis and Deep Learning: Proceedings of ICSADL 2022*. Springer, 2023, pp. 183–193.

[27] W. Brunotte, A. Specht, L. Chazette, and K. Schneider, "Privacy explanations–a means to end-user trust," *Journal of Systems and Software*, vol. 195, p. 111545, 2023.