"Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya

Collins W. Munyendo, Yasemin Acar, Adam J. Aviv
The George Washington University

***Abstract*—The usage of mobile loan applications has proliferated in developing countries. This is due to the ease and speed in which they disburse small loans to users, compared to traditional financial institutions, such as banks, that only offer similar loans based on existing customer relationship or collateral. As mobile loan apps are a relatively new industry, these apps are mostly unregulated and therefore tend to charge extremely high interest rates. Further, they collect and sometimes misuse sensitive user data through the course of verifying customers and ensuring loan repayment, such as users' contacts and SMS communications through the mobile device permission system. Yet, the reasons for usage as well as privacy concerns with these mobile loan apps in the developing world, and specifically in Kenya, remain largely unexplored. To investigate mobile loan apps, we conducted semi-structured interviews ($n = 20$) with loan app users in Kenya, and we find that most users generally have privacy concerns, particularly regarding access to their phones' contacts. However, they often overlook these concerns as this outweighs their need to procure loans. At the same time, we find that users struggle to understand the use of permissions by these mobile loan apps (and mobile apps generally), confirming prior research on comprehension of Android permissions. Our results highlight privacy risks, concerns and behavior with the emerging mobile loan app marketplace in the developing world, and we offer recommendations that can help protect their users' security and privacy, including the need for transparent communication by these apps on how they collect, use and secure their users' data.**

I. Introduction

Access to financial services is crucial for economic growth and has been promoted by the United Nations as fundamental in eradicating poverty and achieving the Sustainable Development Goals [1]. However, according to the World Bank [2], about 1.7 billion adults in the world remain unbanked with no access to the services of a bank or similar financial institutions. The largest proportions of unbanked populations are in developing economies such as in Africa, where more than 50 % of the population lacks access to banking services [3].

While mobile money solutions (services that allow users to send and receive money on their cell phones [4]) have improved financial inclusion, particularly in Sub-Saharan Africa, mobile loan applications have emerged as an easy and straightforward way for many users to access credit as smartphone usage soars in the region [5]. Claiming to improve "financial inclusion" in these communities [6]–[9], mobile loan applications allow users (many without formal credit history) to easily and quickly access loans on their smartphones. These apps do not require collateral or security and solely rely on the self-reported registration information along with data collected from users' smartphones via permissions to offer loans.

Kenya, particularly, has been one of the developing countries that has seen the earliest and perhaps most widespread adoption and usage of mobile loan applications. This has been fueled by the country's huge success of mobile money services such as M-Pesa [4], [9] coupled with growing smartphone adoption [10] that allows users to apply and receive loans from mobile loan applications directly to their mobile phones. Some of the most widely used mobile loan applications such as Tala and Branch began operations in Kenya before diversifying to other developing countries such as India [6].

As this is a relatively new and therefore unregulated industry, mobile loan applications charge extremely high interest rates and often require repayment within shorter durations of time, compared to traditional financial institutions such as banks. Further, they collect significant sensitive data from users via data available on the mobile device, authorized through the phone's permission system. This includes collection of contacts and location as part of verifying and calculating users' credit worthiness [8], [9]. Tala, for example, claims to have repayment rates of more than 90 % achieved through modelling users' routine habits by tracking places they regularly visit, people they frequently contact etc [8].

Despite widely reported privacy concerns [11]–[13], most mobile loan applications claim that users have no concerns, with Shivani Siroya, the founder of Tala, saying "customers have no privacy concerns with Tala as they willingly grant access to their private data through the phone permissions for their credit scores to be developed [8]." Nevertheless, the usage, concerns and behavior with mobile loan applications in the developing world remains largely unexplored.

Our study is therefore aimed at investigating the reasons for usage and concerns with the emerging mobile loan applications in the developing world, specifically in Kenya. We were also motivated to study user understanding and misconceptions with security and privacy and how this influences their usage of these loan apps. We seek to answer three research questions:

RQ1: What are the most common mobile loan apps in Kenya and what permissions do they require?

RQ2: How does user understanding of permissions influence their use of mobile loan apps?

RQ3: What are user concerns, tradeoffs and behaviour when using mobile loan apps in Kenya?

To address our research questions, we conducted semi-structured interviews ($n = 20$) with mobile loan app users in Kenya. The interviews were conducted in July 2021 by one of our researchers who is a native Kenyan. Interviews were conducted remotely through either WhatsApp or direct phone calls as a health precaution against the COVID-19 pandemic. Open-coding revealed that saturation was reached after 15 interviews, with no new themes emerging from the five additional interviews conducted thereafter. We asked participants to indicate all mobile loan apps they had used, before focusing on their most commonly used app for the remainder of the interview. Participants described their reasons for using these apps as well as concerns they had with them. After indicating permissions required by their most commonly used loan app, participants described their understanding of the usage of each permission, followed by concerns and non-concerns with loan apps' access to these permissions. Lastly, participants optionally shared any additional information they had about mobile loan applications.

Mobile loan apps are widely used in Kenya, and our results indicate that they fill a crucial financial gap in the developing world by offering loans to users that otherwise have no formal credit history or collateral. In fact, Tala and Branch, the two most common mobile loan apps, have over 5 and 10 million downloads respectively on Android's Google Play alone. At the same time, we find that common mobile loan apps are permissioned to collect significant sensitive user data, similar to other digital credit lenders [14] previously studied. Each of the eight most common loan apps we explored requires access to users' contacts, SMS, location and storage, while seven require access to users' telephone. While users seem to understand what some of these permissions are used for by these apps, they mostly do not know or misunderstand what most of the permissions are used for, confirming prior work on general comprehension of Android permissions [15], [16].

Contrary to what mobile loan applications postulate [8], an overwhelming majority of users have concerns with mobile loan apps, particularly regarding their privacy. Most participants are particularly worried about these apps' access to their contacts, citing that some of these apps call their contacts when they default in loan repayment; this is in spite of these applications not indicating they will use users' data this way. Participants are also concerned about the high interest rates coupled with short repayment periods offered by mobile loan applications. However, they often overlook these concerns as this outweighs their need to procure the loans.

Our work offers recommendations to regulators, application markets, developers and the research community to protect users of mobile loan apps in the developing world. Local regulators should consider enacting laws, similar to those used to regulate other financial players, to prevent user exploitation for example through high interest rates. Mobile loan apps, on the other hand, need to transparently and accurately inform users how they collect, use and secure their data, perhaps through updates to their privacy policies. App markets should regularly check user reviews on their platforms with the goal of removing apps that are malicious or invade users' privacy while other researchers can analyze the applications we have identified to determine if they adequately secure users' data.

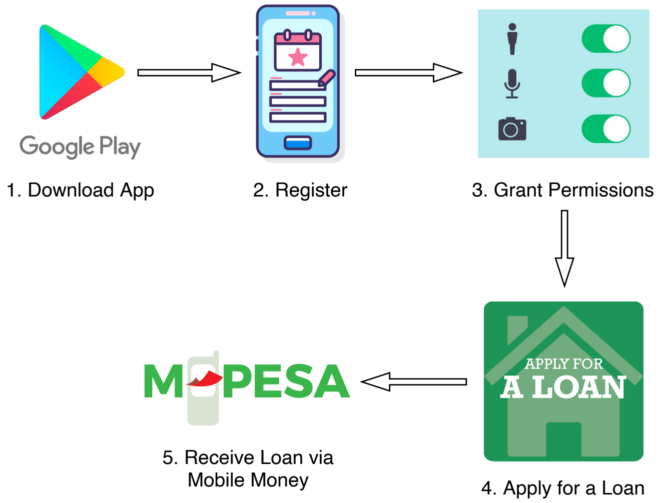


Fig. 1: Loan Procurement Process.

II. Background on Mobile Loan Apps

In this section, we explain what mobile loan applications are and how they work and following, we detail the most common mobile loan apps in Kenya as well as the phone permissions they require. Lastly, we briefly describe how these apps handle users' data as generally explained via their privacy policies.

A. About Mobile Loan Apps

Mobile loan apps are applications that users download from Android's Google Play, Apple's App Store or third-party markets to procure loans. Unlike mobile money services, such as M-Pesa, that allow users to conduct financial transactions on their cell phones [4] for example purchasing goods, paying bills, sending or receiving money, mobile loan apps are solely used to procure loans. Further, they calculate credit scores based on information such as location, contacts or SMS gathered from the prospective borrower's phone [8], [9] through phone permissions. As smartphone usage grows in developing countries [5] such as Kenya [10], these apps have become extremely common due to their speed in disbursing small loans to users coupled with the minimal paperwork or security they require to offer these loans. This is in stark contrast to traditional financial institutions such as banks that require formal credit history or collateral to offer similar loans.

Most mobile loan applications are startups with huge investments from venture capitalists [9] and claim that they are primarily motivated to boost "financial inclusion" in the developing world where most people remain unbanked and lack formal credit history [6]–[9]. Tala, one of the earliest and most common mobile loan apps in Kenya, claims it had lent over $1 billion dollars to more than four million customers spread across three different continents by 2019 [7]. Branch, another common mobile loan app, had over three million customers as well as over 15 million loans issued to customers in Kenya, Nigeria, Tanzania, Mexico and India by 2019 [9]. According to the Kenya Credit Bureaus, more than 19 million

TABLE I: Common Mobile Loan Apps in Kenya.

Loan App	Frequency (%)	Downloads
Tala	14 (70%)	5M+
Branch	13 (65%)	10M+
OKash	8 (40%)	1M+
OPesa	5 (25%)	1M+
Zenka	5 (25%)	1M+
Zash	2 (10%)	1M+
iPesa	2 (10%)	1M+
MoKash	2 (10%)	500K+

TABLE II: Permissions Required by Common Loan Apps.

Permission	Frequency (%)
Contacts	8 (100%)
SMS	8 (100%)
Location	8 (100%)
Storage	8 (100%)
Telephone	7 (88%)
Camera	4 (50%)
Calendar	3 (38%)

Kenyans (about 37% of the population) had used a mobile loan application to borrow money by 2019 [17].

B. How Mobile Loan Apps Work

To use a mobile loan app, a user first downloads the respective app from Android's Google Play, Apple's App Store or other third-party market and installs it on their smartphone. When using it for the first time, the app typically requires the user to register by providing their personal details, mostly demographic and location information as well as their employment details. To verify the customer and calculate their credit score, the app further requires access to the user's phone data through permissions, for example their contacts and SMS.

After registering and granting access to the required permissions, the user can borrow money up to the limit set by the application, with Tala and Branch granting on average $50 to most borrowers [8], [9]. The borrowing process is usually fast, with the money directly disbursed to the user's phone through existing mobile money payment services such as M-Pesa [4] in Kenya. According to Tala [8], users can request and receive loans in under two minutes, and become eligible to borrow even higher amounts upon timely repayment. Further, Tala claims to have high repayment rates, similar to banks, achieved using credit scoring algorithms that analyze and build models of users' routine habits, including tracking their movement through their smartphones' GPS data [8]. Figure 1 shows the loan application process generally, while Figure 3 shows the loan application process for Tala once a user has downloaded and installed the loan application on their smartphone.

C. Common Mobile Loan Apps in Kenya

Kenya is one of the developing countries that has seen the earliest and most widespread usage of emerging mobile loan applications in the world. This is in part due to the huge success of M-Pesa [4], [9], a robust mobile money payment system that allows users to conduct financial transactions on their cell phones [4], as well as growing smartphone adoption in the country [10]. This has attracted several financial technology companies looking to leverage the plethora of user data on smartphones to offer loans to these populations, with a majority of these users otherwise ineligible for loans from traditional financial institutions such as banks due to a lack of formal credit history or collateral.

For this study, we consider a mobile loan application to be common if it is used by at least two participants during our interviews and has at least 500 000 downloads on Android's Google Play. In the end, we had eight common mobile loan applications, with Tala and Branch by far the most common. These apps are used by more than half of the participants in our study. These apps additionally have high download numbers on Google Play, with downloads of over 10 million for Branch, and over 5 million for Tala. Other common mobile loan applications are OKash (8), OPesa (5), Zenka (5), Zash (2), iPesa (2) and MoKash (2). This is summarized in Table I.

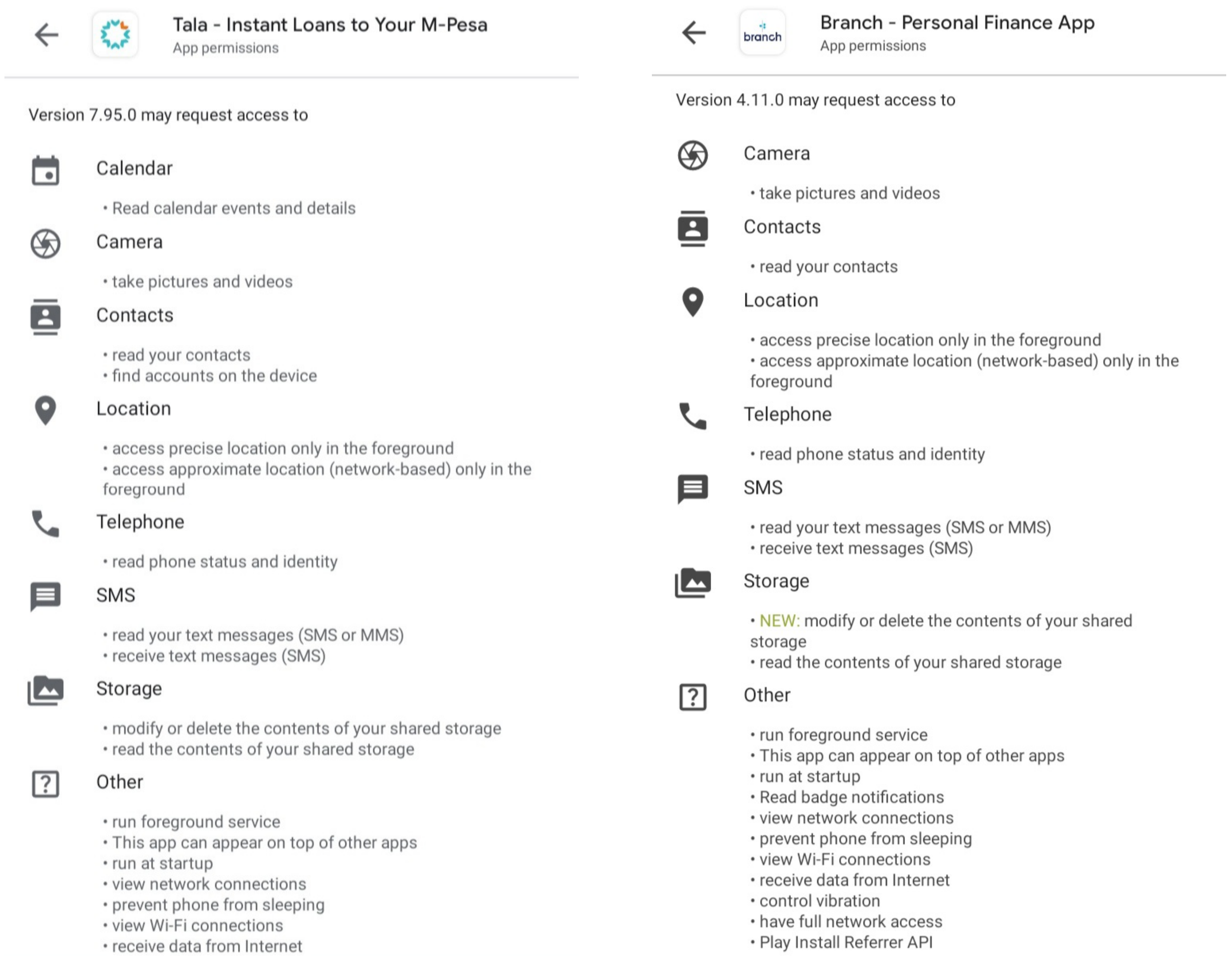
D. Permissions Required by Mobile Loan Apps

To assess customers' ability to pay back loans, mobile loan apps require users to provide their personal information through the registration process as well as grant access to restricted data on their smartphones via phone permissions. By checking Android's Google Play, we find that the most common mobile loan apps in Kenya are permissioned such that they can collect significant sensitive data from users. In fact, each of the eight most common loan applications requires access to users' contacts, SMS, location and storage; seven require access to telephone while four require access to the camera. This has been similarly noted for other emerging digital credit lenders around the world [14] that collect significant, previously undisclosed data types from users.

These results are summarized in Table II, with Figure 2a showing the permissions required by Tala and Figure 2b showing permissions required by Branch. Note, we only focus on Android's run-time permissions as these permissions allow access to sensitive user data; therefore, users must explicitly grant these permissions before their private data is accessed [18]. We do not consider install-time permissions, as they access less sensitive data and are automatically granted when an application is installed on the user's smartphone.

E. Privacy Policies of Mobile Loan Apps

A privacy policy serves to inform users what data is collected from them, the purpose the data is used for and how long the data is retained for a given product or service [19]. Each of the eight common mobile loan applications used by our participants has a privacy policy, with most of them indicating that they collect information from users via the registration details provided, as well as data extracted through phone permissions to compute users' credit worthiness. However, most of these policies are not conclusive. For instance, some participants complain about their contacts getting contacted



Tala - Instant Loans to Your M-Pesa
App permissions

Version 7.95.0 may request access to

Calendar
- Read calendar events and details

Camera
- take pictures and videos

Contacts
- read your contacts
- find accounts on the device

Location
- access precise location only in the foreground
- access approximate location (network-based) only in the foreground

Telephone
- read phone status and identity

SMS
- read your text messages (SMS or MMS)
- receive text messages (SMS)

Storage
- modify or delete the contents of your shared storage
- read the contents of your shared storage

Other
- run foreground service
- This app can appear on top of other apps
- run at startup
- view network connections
- prevent phone from sleeping
- view Wi-Fi connections
- receive data from Internet

(a) Permissions Required by Tala.

Branch - Personal Finance App
App permissions

Version 4.11.0 may request access to

Camera
- take pictures and videos

Contacts
- read your contacts

Location
- access precise location only in the foreground
- access approximate location (network-based) only in the foreground

Telephone
- read phone status and identity

SMS
- read your text messages (SMS or MMS)
- receive text messages (SMS)

Storage
- NEW: modify or delete the contents of your shared storage
- read the contents of your shared storage

Other
- run foreground service
- This app can appear on top of other apps
- run at startup
- Read badge notifications
- view network connections
- prevent phone from sleeping
- view Wi-Fi connections
- receive data from Internet
- control vibration
- have full network access
- Play Install Referrer API

(b) Permissions Required by Branch

Fig. 2: Permissions Required by the Two Most Common Mobile Loan Apps in Kenya.

when they default in payment; this is inspite of the loan apps not indicating they will use this data in this manner. This is similar to Bowers et al.'s findings on emerging digital credit lenders [14] and mobile money services [20] whereby the privacy policies of these services are not only hard to read but also fail to disclose all data collected from users.

III. Methodology

We conducted semi-structured interviews (n=20) to explore user concerns, tradeoffs and behaviour when using mobile loan applications in Kenya. In this section, we discuss the recruitment process, interview procedure, limitations and ethical considerations of our study.

A. Recruitment and Demographics

We recruited (n=20) participants by advertising on Twitter, Facebook and WhatsApp as these platforms are widely used in Kenya. Further, one of the researchers is from Kenya and has a good following on these communication mediums. Snowballing [21] was additionally used whereby participants recommended other people that had used mobile loan applications in Kenya. We restricted mobile loan apps to applications downloaded from the mobile app stores (specifically Android's Google Play) solely for the purpose of procuring a loan, unlike banking or mobile money applications which offer loans to users in some cases, but not as their primary functionality. After open-coding the transcripts, we found that no new themes emerged after 15 interviews, so we should have reached saturation with 20 participants.

To be eligible for the study, participants had to be at least 18 years old and successfully used a mobile loan application in Kenya. Our participants were mostly young (70 % between 18 – 29), well-educated (85 % had a Bachelor's degree or above) and formally employed (75 %). Table III provides the full demographic information of our participants.

TABLE III: Demographics Table.

	Men		Women		Total	
	No	%	No	%	No	%
Age	10	50%	10	50%	20	100%
18-24	0	0%	3	15%	3	15%
25-29	4	20%	7	35%	11	55%
30-34	5	25%	0	0%	5	25%
Prefer not to say	1	5%	0	0%	1	5%
Education	10	50%	10	50%	20	100%
High School	0	0%	1	5%	1	5%
College	1	5%	1	5%	2	10%
Bachelor's	9	45%	7	35%	16	80%
Master's	0	0%	1	5%	1	5%
Background	10	50%	10	50%	20	100%
Technical	5	25%	5	25%	10	50%
Non-Technical	5	25%	5	25%	10	50%
Employment	10	50%	10	50%	20	100%
Student	2	10%	1	5%	3	15%
Self-Employed	0	0%	2	10%	2	10%
Employed	8	40%	7	35%	15	75%

B. Interview Procedure

The interview questions were developed around our research questions described in Section I. Participants first consented to participate in the study before starting the interview. We then asked participants to indicate all mobile loan apps they had previously used and their most used app. The remaining interview questions focused on the participant's most commonly used mobile loan app. We asked participants to describe how the app works, why they use it as well as anything they like and dislike about it. Participants were then asked about concerns they had with this application. If not mentioned, we asked participants about concerns specifically relating to security and privacy. We asked these questions before discussing the application's permissions to avoid priming.

For the second part of the interview, participants were asked to indicate the permissions required by the mobile loan app they had most commonly used by referring to the settings menu on their mobile device. Many participants were no longer using the app and had deleted it from their device. For those, they were directed to Android's Google Play to review the permissions for the application from there.

Participants were asked to describe each permission, what they believed it was used for, and indicate any concern or non-concern for the application using that permission. Lastly, we asked participants if they would behave differently with respect to mobile loan apps as a result of the interview. All the interviews were audio-recorded and conducted in English, one of Kenya's official languages [22]. The full interview protocol and questions can be found in Section A of the Appendix.

C. Data Collection

We piloted our interview procedure with two participants and used their feedback to improve the clarity of our interview questions. We used follow-up questions and deeper probing to allow participants to offer more in-depth information [23]. All interviews were conducted during July 2021. During that time, health precautions against the COVID-19 pandemic were in place, and so we conducted interviews remotely using WhatsApp or direct phone calls, depending on the participants' preferences. Each participant was compensated either 2GB worth of internet data or 125 minutes of call time; this was directly sent to the participant's phone number after the interview. The interviews lasted 21 minutes, on average.

D. Data Analysis

One researcher transcribed and independently coded seven hours of the interview recordings from all participants, developing a primary codebook. To verify its consistency, a secondary coder used this codebook to code half of the interview responses before inter-coder reliability was calculated. Since a good reliability score was not achieved after the first round, the two researchers met to collaboratively update the codebook. After the second round, high agreement [24] ($\kappa > 0.7$) was reached, with the primary codebook used to discuss emerging themes from the study across all the 20 interviews.

E. Limitations

Our study has several limitations. Foremost, some participants indicated they were no longer using mobile loan apps and therefore, they might have been unable to remember some information about them. While some context was lost during these interviews, we were also able to learn about why participants stopped using these applications. Even if the participant was no longer using the mobile loan app, we were able to refresh their memory by directing them to Android's Google Play to review apps they previously used and the permissions requested by those apps.

Another limitation is that this study focused on mobile loan application users on Android only. Many of these apps are available on iOS, but due to the prevalence of Android devices in Kenya [25] and the use of permissions, Android provides the best platform for investigation. Future work may explore these applications on other mobile operating systems.

As is typical with interview studies, our recruited sample size was relatively small. However, we performed open-coding on the collected data and noted that no new themes were emerging after 15 interviews. We conducted an additional five interviews, and ultimately ended data collection after 20 interviews due to saturation. Further, our results are primarily qualitative, and the counts provided in the codebook available in Section A of the Appendix only highlight prevalence of common themes. Thus, they should not be interpreted as an attempt to generalize beyond our sample.

Our recruitment sample also skewed mostly young and educated participants. We do not claim our results to be representative of the general population of Kenya. Further, as is typical with interview studies, a possible lack of anonymity may limit the information shared by participants [26]. To this end, we informed participants that their personally-identifying information would not be recorded as part of the interview. Further, conducting the interviews remotely may have helped in alleviating this concern. Lastly, our study was only conducted with participants from Kenya, and additional work is required to study mobile loan applications in other contexts.

F. Ethical Considerations

This study was approved by our Institutional Review Board (IRB). We fully informed participants about the purpose, duration and associated risks of participating in the study. No personally-identifying information was collected from participants, with all audio recordings immediately transcribed and further de-identified after the interviews. Participants also had the option to withdraw from the interview at any time.

IV. Results

In this section, we discuss the reasons for the usage of emerging mobile loan applications in Kenya as well as user understanding of the phone permissions they require, and following, we discuss user concerns, tradeoffs and behaviour when using these apps. We do not report counts, and those provided in Tables IV, V, VI only add weight to common themes or highlight unique perspectives. However, they should not be interpreted as an attempt to make generalizations.

A. Reasons for Use of Mobile Loan Apps

Most participants use mobile loans apps because of their quick loan disbursement coupled with minimal paperwork required to procure loans in comparison to traditional financial institutions such as banks. For instance, P12 stated that "the good thing with Tala and Branch *[is that]* you get *[the]* money instantly, it doesn't even take, like, five minutes" while P16 indicated that mobile loan applications require less paperwork and are quick in disbursing loans:

> "When you compare *[loans from the apps]* with bank loans; where you will go to the bank, you will see the bank manager, you will be given a form, you need to look for guarantors, you need to attach some particulars, your contract if you are employed, your payslip number. You need to attach maybe your previous three pay slips. You need to get maybe some ID, photocopy for the guarantors and all that. So it may even take a month for you to access that bank loan. But for the mobile loan apps, I can say that they are instant. So long as you are not listed *[with a Credit Reporting Agency]*, so long as you qualify, then you will just download the app, apply *[and]* within five minutes maximum when you are on a good network and you meet the required threshold, you will get the money. They are instant and they help a lot during emergencies."

P11 similarly added that the quick loan disbursement from mobile loan apps is particularly helpful during emergencies:

> "It's quite helpful, especially when you have an emergency as compared to other loans like *[from]* banks. Yeah, because *[with]* banks, they have so many paperwork and processing time is not quite convenient when you're having an emergency."

A few participants mentioned using mobile loan apps because of promotions or recommendations, with P14 stating:

> "It was the most commonly used app on campus. Plus they had this feature; if you refer *[sic]* someone and they used your code, *[and]* they apply for their first loan and pay it *[back]*, they give you 500."

P15 mentioned using loan apps because of the convenience derived from their integration with existing mobile money services such as M-Pesa:

> "It's convenient; that linking between the app and mobile payment; because if you can transact easily to M-Pesa and you know M-Pesa is widely used in Kenya; it's an advantage and also convenient."

Overall, mobile loan applications appear to fill an important financial gap in developing countries by offering small loans to users that would otherwise be ineligible for loans from traditional financial institutions such as banks. This is due to financial institutions requiring formal credit history or collateral which a majority of these users seem to lack.

B. User Perception of their Credit Score Calculation

As mobile loan apps vaguely mention that they compute users' credit worthiness through data collected from users' smartphones via permissions, we asked participants how they think their credit scores are calculated. Our results indicate that most participants do not know how this is performed, with a majority anticipating that their credit score is calculated over time as they borrow and repay the loans. For instance, P11 said "I'm not really sure but one thing I know *[is that]* once you pay *[back]* on time, they will increase your loan limits." Several participants also speculate that the employment details they provide on sign up are used, with P7 stating:

> "They ask for information on how much you earn and also the type of employment; are you a business person? Are you employed? Is the employment permanent or contractual?"

A few participants anticipate that these applications check their credit score on Kenya's Credit Reference Bureau (CRB) [27] while others believe that the apps check their transaction history from their messages due to the prevalence of mobile money services. For instance, P2 said:

> "I think they just check your M-Pesa messages like transactions, because among the first permissions you give them is your messages app."

While several participants correctly allude to mobile loan applications generating their credit scores from the data accessed from their smartphones either during registration or via phone permissions [8], [9], a majority of participants are unsure about this process. This suggests an opportunity for mobile loan applications to genuinely and transparently inform users how their credit scores are calculated to increase trust. This could be through updates to their privacy policies to detail how information is collected and used from users' devices or via transparent communication when requesting permissions.

C. User Understanding of Permissions

As understanding permissions' usage is fundamental in protecting privacy when using mobile apps, we asked participants to explain their understanding of the usage of each permission required by their most frequently used mobile loan app. Note that mobile loan apps indicate that access to these permissions is generally required to calculate users' credit scores.

These results are presented in Table IV. While participants generally have an idea of what some permissions are used for, they do not understand the use of a majority of the permissions. Particularly, most of the participants do not know what the telephone, storage and camera permissions are used for by mobile loan apps, confirming prior research on general comprehension of Android permissions [15].

a) Contacts: A majority of participants believe mobile loan apps use their phones' contacts to follow up on their loan if they default, with P13 saying: "I think it's because, once I default, they can call those people." As access to contacts allows the app to read all the contacts on a user's smartphone, this indicates that most users correctly understand how this permission can potentially be used. Further, as we discuss under concerns in Section IV-D, this has happened to some participants where their contacts are contacted when they default in loan repayment, despite the app not mentioning that this information will be used in this manner. At the same time, a few participants incorrectly indicated that access to their contacts is required for the app to contact the participants themselves. This is incorrect as the applications contact users through SMS or their phone numbers captured from the registration process or via the telephone permission, rather than through their contacts permission.

b) SMS: Most participants believe that loan apps use the SMS permission to check financial transactions on their phones (mostly because of the prevalence of mobile money services such as M-Pesa), send them SMS reminders to pay back loans or just know their frequently contacted people. As the SMS permission can be used to read, send or receive messages to or from the user's smartphone, most users once again provide reasons consistent with this. For instance, P20 mentions that access to their SMS helps the mobile loan apps to calculate their credit worthiness, inline with reasons provided by some of the mobile loan apps themselves [8], [9]:

> "Of course, in your phone, you have M-Pesa messages. They use part of that to gauge how much they can give you and your ability to pay back."

However, P14 incorrectly mentioned that access to their SMS is needed so that the app can send messages to their contacts: "For messages, I think it's because they usually spam your contacts if you don't pay your loan." This is incorrect as these applications send messages directly to users' contacts accessed via the contacts permission, rather than through the participants' SMS.

c) Telephone: While a majority of participants do not know how the telephone permission is used, a few believe it is required for the app to disburse the money to their phone through mobile money services such as M-Pesa. Since this permission allows the app to determine the device's phone number, the app can indeed use this information to send money to the participant's phone number. However, it is evident that users seem unaware that this permission can allow the app to make phone calls, see ongoing call status, redirect calls and even edit call logs on their smartphones. Further, this permission can be misused to monitor a user's phone habits and even make calls without the user's consent.

d) Location: An overwhelming majority of participants believe that access to their location is used by mobile loan apps to track them or confirm the location that they self-report during sign up. For instance, P18 stated that "location is for tracking you if you don't pay" while P8 added that "when registering, you normally say I live in this *[place]* or I am in this *[place]*; so they want to confirm whether it's true or not." Since access to location can allow the app to access the phone's location through GPS, cellular data or WI-FI, most participants seem to correctly know the potential usage of this permission. Only a few participants indicated that they did not know how mobile loan apps use this permission.

e) Storage: While the storage permission can allow an app to access and modify media, photos and other files on the phone's memory, most participants do not know the usage of this permission to mobile loan apps. Only P18 mentioned that this permission allows the app to access files, for example their payslip that might be stored on their phone. A few participants incorrectly mentioned that this permission is required for the app to install on their device. This is wrong as applications do not require access to this permission to be installed. P1 wondered how the loan is related to their phone's storage:

> "How is my storage going to help? The money is not going to eat up my storage. That's so funny."

f) Camera: While most participants do not know what the camera permission is used for by mobile loan apps, several correctly indicated that it is required to capture and upload photos among other documents that might be required as part of the loan application process. Interestingly, most of these participants indicated that the camera can also be used to secretly capture and upload their photos to the loan apps when they are unable to pay back loans, with P20 saying:

> "For the camera, I think as long as you have the app installed and probably you don't pay their loan, I think they use the camera to take a picture of you unknowingly, and probably put it out there so that they can shame you."

g) Calendar: Most participants believe that access to their calendar can help the mobile loan app determine their pay dates, with P1 saying that they "think the reason is to know when you usually get your money." While this is technically correct if users have saved their pay dates on their calendar, this access also allows the app to create, edit and even delete events on the smartphone's calendar which participants did not mention. P12 was apprehensive about the use of their calendar:

TABLE IV: Permissions' Use by Mobile Loan Apps.

Permission	Permission's Actual Use	What Participants Mention the Permission is Used For
Contacts	Read, create, or edit contact list	Call or SMS users' contacts upon defaulting (17) Access or confirm guarantors (3) Call users (2)
SMS	Read, receive, and send MMS and SMS messages	Check transactions (10) Send SMS reminders to pay (5) Know frequently contacted people (4) Check defaults for other loans (2) Phone verification (2) To send messages to users' contacts (1) Send users news updates (1) Promotional texts (1)
Telephone	Access phone number and network information	Don't know (5) Used to send the users money (3) Reminder calls (3) Track users (2) Confirm phone ownership (2) Check frequently contacted people (1) Check phone type (1) Call users' contacts (1) Promotional calls (1)
Location	Access location using GPS, cellular data or Wi-Fi	Track users (14) Confirm location against the one provided during sign up (5) Don't know (2) Customize services (1)
Storage	Access files, media, or photos on the phone's memory	Don't know (12) For app installation or storage of installation files (3) Install backdoor (1) Access files (1) Check other apps on the phone (1)
Camera	Take photos, record footage or stream video	Don't know (7) Take photo or upload documents (6) Assess or judge users' ability to pay based on looks (3) Spy on users (1) Track users (1)
Calendar	Read, create, edit, or delete calendar events	Know users' pay date (5) Record keeping (2) Locate users (1) Know borrowing date (1) Don't know (1)
Microphone	Record audio, including for video	Talk to an agent via the app (2) Don't know its use (2) Record users (1)

> "Honestly, I would ask you the same question. Why do they need my calendar? It's not like my calendar is the one that's going to pay for the defaulted loan. So why do they need it? It doesn't make sense."

h) Microphone: For the five participants whose commonly used mobile loan application required access to their microphone, a majority correctly mentioned that the microphone can be used to either speak to an agent via the app or record them. Only few participants were unsure about its use to the app, with P10 saying: "I am not sure why they access my microphone because there is nothing that requires the microphone when using the app that I have ever experienced."

Overall, while users seem to have a good idea of how some of the permissions are used, they either do not know or have incorrect understanding of how most of the permissions are potentially used. This confirms prior work [15], [16] that has shown that users generally struggle to comprehend Android permissions, despite vast design improvements [18].

D. User Concerns with Mobile Loan Apps

When asked about concerns they had with mobile loan applications, participants provided a variety of responses ranging from high interest rates charged on loans to security and privacy concerns. These are discussed below.

a) Concerns with Loans: A majority of participants were concerned about the high interest rates that are charged by mobile loan applications when offering loans, with P1 saying "their interest *[rate]* is so high, as much as 20 %." P9 added that "comparing them to maybe banks or SACCOs, or any other financial institutions, you find that their interest *[rates]* tend to be extremely high." Several participants further complained about growing interest rates or penalties when they fail to repay the loans on time, with P16 saying "they do increase their loan if you default to pay within an agreed period of time." Other concerns relating to loans mentioned by participants include the short repayment period offered, with P8 stating that "the duration required for payment is usually not that sufficient." Some participants complained about these applications deducting interest upfront before disbursing the loans to them, while one participant mentioned that the loan amounts offered by these applications are negligible.

These results suggest the need for regulation of mobile loan applications. Unlike traditional financial institutions such as banks which are well regulated in terms of their interest rates and other repayment terms, mobile loans apps are relatively new and lack proper regulations. This unfortunately leads them to exploit vulnerable customers who are unable to secure loans from traditional financial institutions due to a lack of collateral or formal credit history. Fortunately, promising regulations are starting to emerge for example in Kenya [28], to protect users of mobile loan applications.

b) Concerns (and Lack Thereof) with Permissions: After participants had reviewed all the permissions required by their most commonly used mobile loan application, we asked them which permissions were concerning and non-concerning to them. Table V summarizes the permissions participants were concerned about.

TABLE V: Concerning Permissions.

Permission	Reasons For Participant Concern
Contacts	Contacts not involved in loan procurement (9) Name defamation by calling contacts (5) Contacts will be threatened upon defaulting (5) Only guarantors should be contacted (4) Contacts will be tracked (1)
Camera	App will use it to spy on participants (3) Don't know its use to the app (2)
SMS	App will read participants' private messages (2)
Location	App will track participants (2)
Storage	App will misuse storage (1) Don't know it's use to the app (1)

Almost all participants were concerned with these apps' access to their contacts, with a majority uncomfortable with these apps contacting and sometimes harassing their contacts when they default. For instance, P1 stated:

> "They will start calling your parents or they'll start calling your brothers and sisters because they've got your contacts. They've seen whatever the contacts that you have, they just call anyone, even someone that is not into that business of you borrowing or not borrowing. They will tell them that this person has taken money from us, he is stealing from us. So you get *[that]* they've tainted your name trying to blackmail you so that you can pay back their money, as much as your intentions were not to steal."

P8 was particularly worried about their contacts getting threatened when they default in repayment, even though most of these contacts are not provided as guarantors for the loan:

> "They get in touch with them and threaten them, telling them to ask the loan applicant to pay the amount or they will access that person's phone and deduct that amount from them; and yet, you hadn't listed that person as a guarantor."

P11 narrated how one app contacted their father-in-law when they once defaulted, making them embarrassed:

> "They called my father-in-law. Do you know someone called *[participant name?]* Remind her to pay our loan worth 6 000. Then they also sent him countless messages. I felt bad and embarrassed. I had to apologise to my father-in-law."

Several participants indicated they were worried about getting spied on because of these apps' access to their camera, with P12 saying "I feel like I am being spied on." Some participants also indicated concern with access to their location due to fear of being tracked while some other participants were concerned about these apps reading their private conversations through the SMS permission. For instance, P15 asked "why would they want to read my messages?"

Table VI shows the permissions that participants were unconcerned about. Surprisingly, several participants said they were not concerned with these apps' access to their storage, telephone and camera permissions as they did not understand what these permissions are used for by the loan app. For instance, P19 said they were unconcerned about storage because they "don't know the reason for allowing the permission" while P4 was unconcerned about "telephone because I have not really understood why they need that."

Several participants indicated being unconcerned with access to their location as they believe it's a legitimate way for the mobile loan applications to follow up with them if they default in repayment of the loan. For instance, P13 stated:

> "I don't think they have collateral; if you fail to pay them and disappear, they will undergo a loss. So I really think that the location *[permission]* is okay. You can't just take a loan and decide to disappear. I think this is a good technique on how they can follow up on the loan."

Generally, the few participants that were unconcerned with loan apps' access to their contacts, camera and storage permissions believed these applications had legitimate reasons to access this information, similar to their location. For instance, P2 was okay with access to their contacts as they believe this would provide a valid way for the app to access the guarantors provided for the loan: "I understand when they want to access your contacts because they probably want to check

TABLE VI: Non-Concerning Permissions.

Permission	Reasons For Non-Concern
Location	Used to verify geographical eligibility (3) Participant can easily move (3)
Storage	Don't know its use to the app (5) Required for the app to install (1)
Camera	Don't know its use to the app (2) Necessary to upload photos or documents (1) Remove the app immediately after use (1)
Telephone	Don't know its use to the app (2) App has it already (1)
Calendar	Nothing important stored on calendar (1) Don't know its use to the app (1)
Contacts	Contacts are publicly available (1) To confirm the guarantors provided (1)
SMS	Have no private messages in SMS (1) Comfortable receiving app's messages (1)
Microphone	Never used the mic in the app (1)

if the guarantor's name is legitimate, *[and]* if the *[guarantor's phone]* number is working."

At the same time, some participants were unconcerned with access to certain permissions if they believed they had workarounds to secure their privacy or had no private information on their devices. This was particularly the case with calendar and SMS permissions whereby P7 mentioned they do not have anything important on their calendar nor any private messages in their SMS. P20 was unconcerned with access to their camera as they immediately uninstall the app after use, while some participants were unconcerned with access to their location as they can move to different places anytime to avoid getting tracked by these applications.

Generally these results indicate that users have several privacy concerns regarding access to their data via permissions by loan apps. Similar to prior research [29], [30], users seem more concerned about access to their contacts, but less so with their storage. However, they are willing to grant access if they believe the permissions are legitimately required by the app. This suggests a need for loan apps to strictly request permissions that are necessary to their operations. Further, they need to transparently indicate the reason for requiring each of the permissions, perhaps at the time of requesting this access.

c) Security and Privacy Concerns: Besides concerns with permissions, participants mentioned additional security and privacy concerns with these apps. Some participants were concerned about their private information being shared with third parties as part of the loan recovery process, with P9 saying that "in the case whereby you don't pay the loan on time, they tend to give your information to some third parties." P20 was worried that these apps provide no option to delete their information: "One thing I don't like is that they don't give you an option to opt out and for them to sort of delete or do away with your data." P19 on the other hand was worried that they do not know how their information is used: "All that information, how it is used or where it goes, I don't know."

d) Other Concerns: Apart from security and privacy, more than half of participants were concerned about borrowing addiction or temptation stemming from easy access to loans provided by mobile loan apps. P19 described how they have to constantly borrow from some other loan apps just to pay off loans from other mobile loan apps:

> "You are ever in a debt cycle; you have to borrow from this one app to repay this app before the time expires, and then the cycle continues that way; you borrow from this app, pay the other app, borrow again. The time comes, borrow from this app, pay again. And then the cycle continues that way."

Lastly, some participants indicated concern with getting listed with Kenya's Credit Records Bureau (CRB) [27] upon defaulting, limiting their ability to procure loans or even get employed in future. For instance, P9 stated:

> "When you don't pay back, definitely they register you with CRB. Yeah, so of course when you are registered with CRB, you know, you can't access any other loan anywhere."

Public outcry about the misuse of CRB's Credit Information Sharing system by mobile loan applications led the Central Bank of Kenya to temporarily suspend mobile credit lenders from listing customers who had defaulted in loan repayment to CRB from April to September, 2020 [31]. To be allowed to report customers that default, mobile loan companies must now meet certain stipulations including detailing their technical staffing as well as credit providers [32]. This has been a promising step in alleviating some of the concerns relating to CRB mentioned by some of our participants.

E. Privacy vs Loan Tradeoffs

After reviewing all the permissions required by their most commonly used mobile loan app, we asked participants if they were comfortable granting these apps access to all these permissions. Half of the participants were uncomfortable, but would still grant the permissions in order to procure the loans. For instance, P1 said that "the funny thing is when you need money, you won't care about privacy issues" while P13 added that they were worried they would be denied the loan if they did not grant access to all the required permissions: "Sometimes I'm not comfortable, but sometimes you see, you might disagree and then they might not give you the loan." P11 was unsure what these apps do with all the access they have to their information:

> "You don't know what they want to do with them *[users' data]*. But again, they say desperate times call for desperate measures. You need the cash, you don't have an alternative."

P16 was unaware these apps had that much access to their data: "So I had no idea and I had no otherwise because I was in need of money" while P2 added that they would not grant any of the permissions if they had a choice: "If it were up to me, I wouldn't even give them access to anything."

F. User Behaviour and Suggestions

At the end of the interview, we asked participants if they would do anything differently with mobile loan apps as a result of the interview. We further asked if they had any other information they wanted to share about these apps. Several participants indicated that they would either avoid these apps all together after learning about the access they had via permissions, or would be more careful when using them in future. P4 was shocked about how much sensitive data these apps accessed, saying they would not use them again: " I don't think I will go back to using the mobile loan apps once I have learned about all the access that they require." P13 said they would do some research around the permissions required by these apps: "I will try to research about the permissions because I really didn't know about them."

Some participants indicated a need for mobile loan apps in Kenya to be regulated when asked to share any additional thoughts about these apps. P20 acknowledged the convenience they bring but mentioned a need for regulation of both their interest rates and data collection practices:

> "Apart from the convenience they bring, if something probably could be done in terms of regulation; on how to go about let's say regulating them in terms of their rates; because they have pretty high interest rates. Then again, something about controlling the amount of data they can access from you."

P15 suggested the need for data protection regulations in Kenya, similar to those used in Europe, to prevent mobile loan apps from accessing more data than they need:

> "I don't know who controls issues of data privacy in Kenya or anywhere else, I probably should think they should have control. Like we have issues of GDPR in Europe. If they have that implementation in Kenya, it would be good, because I think they are accessing more than what they need."

Overall, while these results show that mobile loan apps provide quick and useful loans to many borrowers in Kenya who lack access to credit from other financial institutions, they highlight several privacy and security concerns that these applications pose to the sensitive user data they collect as part of verifying customers and ensuring loan repayment. Specifically, these applications need to transparently and accurately inform users how they collect, use and secure their data, perhaps through updates to their privacy policies. They can also offer transparent explanations of the use of run-time permissions when they request them. Further, these apps need to be regulated, similar to other financial institutions such as banks, to prevent them from exploiting their customers for example through high interest rates.

V. Discussion

In this paper, we explore user concerns, tradeoffs and behaviour with emerging mobile loan applications in the developing world through semi-structured interviews ($n = 20$) with users of these apps in Kenya. Generally, we find that most users have privacy concerns with these apps. However, they often overlook these concerns in order to procure loans.

In the rest of this section, we discuss broader themes that emerged from our study, and offer recommendations that can help protect the security and privacy of this largely unexplored user demographic.

a) Importance of Loan Apps in the Developing World: Our results highlight the important financial gap that mobile loan applications seem to fill in developing countries. As many people in these populations remain unbanked often with no formal credit history or collateral, mobile loan applications provide their best chance to access credit that can be used to meet their personal financial needs or fund their enterprises. Therefore, with proper legal frameworks, for example those used to regulate other players in the financial industry such as banks, these applications can improve financial inclusion in these communities while not exploiting their customers, for example through high interest rates or misuse of their data. Such regulations are promising, and are already being discussed and advanced in countries such as Kenya [28].

b) Concerns with Mobile Loan Apps: Despite benefits in enabling many unbanked people access loans, our interviews reveal strong resentment from users towards these applications from a privacy perspective. This is because these apps collect significant sensitive user data through phone permissions as part of verifying and generating users' credit scores. At the same time, they seem to either misuse or fail to accurately inform users how this data is used, with some participants mentioning that their contacts are called when they default in repayment, despite the apps not mentioning they will use their data this way. This is contrary to what most mobile loan applications postulate, with the founder of Tala, a popular loan app, claiming that users have no privacy concerns with Tala [8]. To this end, mobile loan applications need to transparently inform users how they collect, use and secure their sensitive data. This can be through improvement of their privacy policies to detail why they collect and how they use different data from their users, instead of vaguely stating that the data is used to calculate users' credit worthiness. Relevant government and industry regulation can play a big role in enforcing this, as similarly recommended by Bowers et al. [20] for mobile money services around the world.

c) Privacy vs Loan Tradeoffs: While a majority of participants indicated privacy concerns with mobile loan applications, most of them overlook these concerns to procure loans. This is not surprising as prior work [33], [34] suggests that users tend to choose convenience over privacy or security. Nonetheless, consequences from privacy malpractices by some of these applications can be far reaching. For instance, when these applications call users' contacts without informing them, they breach the privacy of the users themselves as well as their contacts who were not even involved in procuring the loan in the first place. Therefore, application markets should consider removing applications that outright invade users' privacy from their stores. A good starting point would be regularly checking user reviews for these applications on their platforms, and further investigating and possibly removing applications that seem to infringe on users' privacy.

d) (Mis)understanding of Permission Use: Despite design improvements for Android permissions [18], we find that many users still misunderstand or do not know what certain permissions are used for by mobile loan apps, confirming prior work [15], [16] on general comprehension of Android permissions. Particularly, most users do not understand what the telephone and storage permissions are used for. Strikingly, users seem unconcerned with access to these permissions because of being unaware about how they are used. Nonetheless, Android should consider using names that are more easily understood by users in regards to the permissions, as users seem to better understand permissions such as contacts, SMS and location, perhaps more so than storage and telephone.

e) User Education: After learning about the sensitive data that mobile loan applications access on their smartphones, several participants indicated they would either avoid these applications all together or would be more careful when using them in future. This suggests that educating users about security and privacy is a promising way to guide them towards better security behaviour. This could be through trainings at institutions as well as using advocates to create more security awareness, as recommended by Haney and Lutters [35].

f) Over-privilege of Mobile Loan Apps: Prior work [36]–[38] has shown that a majority of mobile applications request unnecessary permissions either to gather valuable user data or because of developer errors. Similarly, our study finds that the most common mobile loan applications in Kenya collect significant sensitive user data through phone permissions, with the most common loan apps requiring access to users' contacts, SMS, location and storage. While they claim to use this information to calculate users' credit worthiness [8], [9], some of these apps end up misusing this information. While prior work [39], [40] recommends that mobile applications should provide contextual information when requesting run-time permissions to improve transparency, our results indicate that loan app users' motivation to get loans far outweighs their privacy concerns. Therefore, application markets can once again play an important role by investigating and removing invasive apps from their stores to protect the privacy of not just loan app users, but all their users in general. Mobile loan app developers, on the other hand, should follow the least privilege approach recommended by Android [18] and only collect user data that is necessary to their operations.

g) Recommendations: Our results highlight concerns, tradeoffs and behaviour with emerging mobile loan applications in the developing world, and we offer recommendations to regulators, application markets as well as the broader research community to protect the security and privacy of this largely understudied user group. Local law-makers should particularly enact laws, similar to those that regulate other financial institutions such as banks, to prevent users from getting exploited with these applications for example via high interest rates or unreasonably short repayment periods. They should also create relevant data protection laws to protect users. Application markets should consider automated ways to check user reviews of applications on their stores with the goal of detecting apps that are malicious or violate users' privacy. Once flagged, these applications can be further investigated and removed from the stores if they indeed are privacy-invasive or pose security risks to their users as well as their data. As part of future work, other researchers can statically and dynamically analyze the applications we have identified to determine if they engage in security best practices to further protect users; this was outside the scope of our study.

VI. Related Work

Android permissions allow users to control information that can be accessed on their devices by mobile applications [18], [41]. This could be reading data on the device such as contacts and SMS, all the way to accessing hardware features such as the device's camera or microphone. Android categorizes permissions into three broad categories; install-time, run-time and special permissions. Install-time permissions give an application access to less sensitive data and are automatically granted to the application when it is installed. Run-time permissions, also known as dangerous permissions, give access to more sensitive user data, and require explicit user approval [18], [42] before they can access the user's data. Special permissions, on the other hand, correspond to specific application operations and can only be defined by the Android platform itself. Throughout our study, we focus on run-time permissions as they access sensitive data and require direct user approval before they can access users' data.

Prior work has explored user understanding of Android permissions. Through a usability study, Felt et al. [15] found that most users pay less attention to permission warnings in addition to not properly understanding how different permissions are used. Kelley et al. [16] confirmed these results, finding that users generally view and read Android permissions, but do not understand them. They additionally found that users are unaware of the security risks posed by mobile applications due to overly trusting the application markets. Despite several improvements [18] to Android since then, our study similarly finds that users still struggle to understand the use of certain phone permissions, notably their telephone and storage.

Users' willingness to grant and deny permissions to apps has also been explored, with Jialiu et al. [43] finding that users' inclination to grant a given permission to a mobile application is strongly influenced by the purpose associated with such a permission. This is also reflected in our study whereby users are unconcerned about access to permissions they believe are legitimately required by the mobile loan application.

Other studies have explored the permissions required by Android applications. Khatoon et al. [36] studied the different ways in which applications gain access to sensitive device permissions when installed on Android, finding that many free apps tend to request unnecessary permissions to gather valuable user data. Chia et al. [44] found that free apps and apps with mature content request more permissions than is typical across Facebook applications, Chrome extensions and

Android applications. Additionally, they found that popular applications request more permissions than average. Our study observes a similar phenomenon with common mobile loan applications in Kenya, with these apps collecting significant sensitive user data via permissions to verify and calculate users' credit worthiness when offering them loans.

Tools have been developed to check if mobile applications use the permissions they require. Felt et al. [41] built a tool called Stowaway to detect if Android applications require more permissions than they actually need, establishing that about a third of the applications they studied were over-privileged. Interestingly, they found evidence that developers were trying to follow the least privilege approach but occasionally fail due to insufficient documentation. Johnson et al. [38] developed an architecture to map Application Programming Interface (API) calls of Android applications to their required permission(s), finding that most application developers do not use correct permissions sets for their applications. This often leads to either over- or under-privileged applications.

Additional tools have been developed to enable users make better privacy decisions. Liu et al. [45] developed a personalized privacy assistant for mobile app permissions and found that not only were their recommendations followed by users but also spurred them to review and modify their permission settings using daily nudges. Kelley et al. [46] found that by bringing privacy information to users when they are making decisions and in a clearer way, users can be assisted in choosing applications that request fewer permissions. Wijesekera et al. [40], [47] and Tsai et al. [48] have recently shown that users' decisions regarding the granting or denial of permissions are contextual, and that machine learning can be used to assist them to make better privacy decisions.

More recent work on Android permissions has been conducted by Almomani and Khayer [37]. By analyzing Android permissions since Android's inception in 2008 to 2020, they find that permission categories have been continuously increasing on the Android platform. This is also reflected in Android applications, with several applications increasing their permission usage by over 70 %. Despite several design improvements to the Android Operating System [18], Almomani and Khayer still find over-privilege as a persistent challenge with most Android applications, consistent with our findings on common mobile loan applications in Kenya which request for significant sensitive data from users through permissions.

Beyond permissions, security and privacy behaviour has been shown to vary across countries and cultures [49]–[51], suggesting the need for more tailored security and privacy solutions for the target users. Daffalla et al. [52] found that security and privacy recommendations do not always generalize to all user groups through their study of technology usage by political activists in Sudan, while Reichel et al. [53] found differences between privacy behavior of Facebook users in South Africa compared to western societies. Other studies have explored vulnerable populations including journalists [54], undocumented immigrants [55], human trafficking survivors [56], refugees [57], protesters [58], children [59], [60], older adults [61]–[67], sex workers [68], [69] and women in South Asia [70], revealing unique challenges that are not readily solved by broader security and privacy solutions. Our work builds on this promising line of research by exploring privacy concerns, tradeoffs and behaviour with mobile loan apps in the developing world. Our results and recommendations contribute to improved security and privacy for this user group, as well as other broader populations.

Our work is most closely related to the research conducted around online credit lenders [14] and mobile money services [20], [71] by Bowers et al. and Reaves et al. Through a comprehensive security analysis of emerging online credit lenders around the world, Bowers et al. [14] found that these applications collect previously undisclosed data types as well as insecurely handle this data. Bowers et al. further found that these applications' privacy policies are not only hard to read, but do not mention all data that is collected from users. Through another study, Bowers et al. [20] studied privacy policies of mobile money services. Unlike the online credit lenders, they found that almost half of mobile money services do not have a privacy policy. For apps with existing policies, they similarly found that these policies are either too hard to read for their target audiences or clearly fail to show what user information is collected and how it is stored. Through a related study, Reaves et al. [71] uncovered multiple vulnerabilities with Android mobile money applications, including information leakage that can allow attackers to modify transactions and even steal funds. Our study confirms and expands on some of these findings, specifically focusing on mobile loan applications in Kenya. Unlike Bowers et al. and Reaves et al., we leverage a user-centric approach through semi-structured interviews with users of these applications to show, for the first time, user concerns, tradeoffs and behaviour when using mobile loan applications in the developing world.

VII. Conclusion

As smartphone usage grows in developing countries, mobile loan applications have become a popular way for many users to access credit, with a majority of them otherwise unable to procure loans from traditional financial institutions such as banks due to a lack of formal credit history or collateral. However, to verify customers and calculate their credit worthiness, these applications collect significant sensitive data from users including contacts and SMS via phone permissions. Further, they charge extremely high interest rates. Inspite of this, user concerns, tradeoffs and behavior with these applications' use in the developing world, and particularly in Kenya remains largely unexplored. Through semi-structured interviews ($n = 20$) with mobile loan app users in Kenya, we found that mobile loan apps provide useful loans to many users in Kenya, but unfortunately pose privacy risks to users' data. At the same time, a majority of users indicated overlooking these concerns to procure loans. We offer recommendations to regulators, developers, app markets and the broader research community that can help protect the security and privacy of mobile loan application users in the developing world.

Acknowledgment

We thank Darika Shaibekova for her assistance with qualitative coding, as well as June Leiro, Timothy Wood, John Munyi, Hunter Dyer, Joreen Arigye, Lilian Mutua, Karen Mani and Nelson Jaimes for useful discussions about this topic. We also thank all the anonymous reviewers for their insightful comments and feedback. Lastly, we are very grateful to all our participants for their time and invaluable insights. This material is based upon work supported by the National Science Foundation under Grant No. 1845300.

References

[1] UN, "Igniting SDG progress through digital financial inclusion," 2018, https://sustainabledevelopment.un.org/content/documents/2655SDG_Compendium_Digital_Financial_Inclusion_September_2018.pdf.

[2] M. Felsenthal and R. Hahn, "Financial inclusion on the rise, but gaps remain, Global Findex database shows," Apr 2018. [Online]. Available: https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows

[3] L. Ventura, "World's most unbanked countries 2021," Feb 2021, https://www.gfmag.com/global-data/economic-data/worlds-most-unbanked-countries.

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

[5] J. C. Aker and I. M. Mbiti, "Mobile Phones and Economic Development in Africa," *Journal of Economic Perspectives*, vol. 24, no. 3, pp. 207–32, September 2010.

[6] Z. Faux, "Tech Startups Are Flooding Kenya With Apps Offering High-Interest Loans," Feb 2020, https://www.bloomberg.com/news/features/2020-02-12/tech-startups-are-flooding-kenya-with-apps-offering-high-interest-loans.

[7] A. Hecht, "2.5 billion people around the world don't have a credit score-here's why that's a problem," Aug 2019, https://www.cnbc.com/2019/08/22/tala-aims-to-help-anyone-with-an-android-phone-have-access-to-loans.html.

[8] S. Adams, "How Tala Mobile is using phone data to revolutionize microfinance," Sep 2016, https://www.forbes.com/sites/forbestreptalks/2016/08/29/how-tala-mobile-is-using-phone-data-to-revolutionize-microfinance/?sh=c3bf17e2a9f2/.

[9] S. Hansen, "Mobile lending App Branch partners with Visa, announces $170 million in fresh funding," Apr 2019, https://www.forbes.com/sites/sarahhansen/2019/04/07/mobile-lending-app-branch-partners-with-visa-announces-170-million-in-fresh-funding/?sh=4bfcd60a3e90/.

[10] J. Poushter, "Smartphone ownership and internet usage continues to climb in emerging economies," *Pew Research Center*, vol. 22, no. 1, pp. 1–44, 2016.

[11] M. Kiruga, "This lending app publicly shames you when you're late on loan payment," May 2020, https://restofworld.org/2020/okash-microlending-public-shaming/.

[12] A. Roussi, "Kenyan borrowers shamed by debt collectors chasing Silicon Valley loans," Sep 2020, https://www.ft.com/content/16c86479-e88d-4a28-8fa4-cd72bace5104.

[13] W. Mwaura, "Kenya outrage over debt collectors' shaming tactics," Aug 2021, https://www.bbc.com/news/world-africa-57985667.

[14] J. Bowers, I. N. Sherman, K. R. B. Butler, and P. Traynor, "Characterizing Security and Privacy Practices in Emerging Digital Credit Applications," in *WiSec 2019: Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[15] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," in *SOUPS 2012: Symposium on Usable Privacy and Security*, 2012.

[16] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone," in *FC 2012: Financial Cryptography and Data Security*, 2012.

[17] CryptoGuru, "19 Million Kenyans Have Active Mobile Loans with 40% Being Multiple Mobile Lenders," Mar. 2019, https://bitcoinke.io/2019/03/19-million-kenyans-active-mobile-loans-40-percent-multiple-mobile-lenders/.

[18] "Permissions on Android," Oct 2021, https://developer.android.com/guide/topics/permissions/overview.

[19] G. Karjoth and M. Schunter, "A privacy policy model for enterprises," in *CSFW 2002: IEEE Computer Security Foundations Workshop*, 2002.

[20] J. Bowers, B. Reaves, I. N. Sherman, P. Traynor, and K. Butler, "Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services," in *SOUPS 2017: Symposium on Usable Privacy and Security*, 2017.

[21] B. Gardner, "Incentivised snowballing," *The Psychologist*, vol. 22, no. 9, pp. 768–769, 2009.

[22] N. O. Ogechi, "On language rights in Kenya," *Nordic Journal of African Studies*, vol. 12, no. 3, pp. 19–19, 2003.

[23] D. Cohen and B. Crabtree, "Qualitative research guidelines project," Jul 2006, http://www.qualres.org/.

[24] C. O'Connor and H. Joffe, "Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines," *International Journal of Qualitative Methods*, vol. 19, 2020.

[25] M. M. Masika, G. B. Omondi, D. S. Natembeya, E. M. Mugane, K. O. Bosire, and I. O. Kibwage, "Use of mobile learning technology among final year medical students in Kenya," *Pan African Medical Journal*, vol. 21, no. 1, 2015.

[26] B. Saunders, J. Kitzinger, and C. Kitzinger, "Anonymising interview data: challenges and compromise in practice," *Qualitative Research*, vol. 15, no. 5, pp. 616–632, 2015.

[27] L. Tuwei, W. Sakataka, and E. Oteki, "Credit reference bureau as the factor influencing the profitability of commercial banks in Kenya: A case of Standard Chartered Bank, Kenya," *International Journal of Novel Research in Marketing Management and Economics*, vol. 2, no. 3, pp. 122–129, 2015.

[28] A. Njanja, "Kenya cracks down on digital lenders over data privacy issues," Oct 2021, https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/.

[29] P. Andriotis, S. Li, T. Spyridopoulos, and G. Stringhini, "A Comparative Study of Android Users' Privacy Preferences Under the Runtime Permission Model," in *HAS 2017: Human Aspects of Information Security, Privacy and Trust*, 2017.

[30] P. Andriotis and A. Takasu, "To Allow, or Deny? That is the Question," in *HCI-CPT 2020: HCI for Cybersecurity, Privacy and Trust*, 2020.

[31] O. Guguyu, "337 digital mobile lenders ejected from CRB listing," Oct 2020, https://www.businessdailyafrica.com/bd/markets/market-news/337-digital-mobile-lenders-ejected-from-crb-listing-2463294.

[32] J. Mbati, "Loan apps given new standards on CRB listing," Jun 2020, https://www.kenyans.co.ke/news/65629-loan-apps-given-new-standards-crb-listing.

[33] M. Sleeper, T. Matthews, K. O'Leary, A. Turner, J. P. Woelfer, M. Shelton, A. Oplinger, A. Schou, and S. Consolvo, "Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy," in *CHI 2019: ACM Conference on Human Factors in Computing Systems*, 2019.

[34] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception," in *SOUPS 2014: Symposium on Usable Privacy and Security*, 2014.

[35] J. M. Haney and W. G. Lutters, "It's Scary…It's Confusing…It's Dull: How Cybersecurity Advocates Overcome Negative Perceptions of Security," in *SOUPS 2018: Symposium on Usable Privacy and Security*, 2018.

[36] A. Khatoon and P. Corcoran, "Android permission system and user privacy — A review of concept and approaches," in *ICCE 2017: International Conference on Consumer Electronics*, 2017.

[37] I. M. Almomani and A. A. Khayer, "A Comprehensive Analysis of the Android Permissions System," *IEEE Access*, vol. 8, pp. 216 671–216 688, 2020.

[38] R. Johnson, Z. Wang, C. Gagnon, and A. Stavrou, "Analysis of Android Applications' Permissions," in *SERE-C 2012: IEEE International Conference on Software Security and Reliability Companion*, 2012.

[39] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android Permissions Remystified: A Field Study on Contextual Integrity," in *Security 2015: USENIX Security Symposium*, 2015.

[40] P. Wijesekera, A. Baokar, L. Tsai, J. Reardon, S. Egelman, D. Wagner, and K. Beznosov, "The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences," in *S&P 2017: IEEE Symposium on Security and Privacy*, 2017.

[41] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, “Android Permissions Demystified,” in *CCS 2011: ACM Conference on Computer and Communications Security*, 2011.

[42] R. Triggs, “Android app permissions explained and how to use them,” Oct 2021, https://www.androidauthority.com/app-permissions-886758/.

[43] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, “Modeling Users’ Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings,” in *SOUPS 2014: Conference on Usable Privacy and Security*, 2014.

[44] P. H. Chia, Y. Yamamoto, and N. Asokan, “Is This App Safe? A Large Scale Study on Application Permissions and Risk Signals,” in *WWW 2012: International Conference on World Wide Web*, 2012.

[45] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, “Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions,” in *SOUPS 2016: Symposium on Usable Privacy and Security*, 2016.

[46] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as Part of the App Decision-Making Process,” in *CHI 2013: ACM Conference on Human Factors in Computing Systems*, 2013.

[47] P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, K. Beznosov, and S. Egelman, “Contextualizing Privacy Decisions for Better Prediction (and Protection),” in *CHI 2018: ACM Conference on Human Factors in Computing Systems*, 2018.

[48] L. Tsai, P. Wijesekera, J. Reardon, I. Reyes, S. Egelman, D. Wagner, N. Good, and J.-W. Chen, “Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences,” in *SOUPS 2017: Symposium on Usable Privacy and Security*, 2017.

[49] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, and A. Yamada, “Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior,” in *CHI 2017: ACM Conference on Human Factors in Computing Systems*, 2017.

[50] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, “International Differences in Information Privacy Concerns: A Global Survey of Consumers,” *The Information Society*, vol. 20, no. 5, pp. 313–324, 2004.

[51] H. Cho, M. Rivera-Sánchez, and S. S. Lim, “A multinational study on online privacy: global concerns and local responses,” *New Media & Society*, vol. 11, no. 3, pp. 395–416, 2009.

[52] A. Daffalla, L. Simko, T. Kohno, and A. G. Bardas, “Defensive Technology Use by Political Activists During the Sudanese Revolution,” in *S&P 2021: IEEE Symposium on Security and Privacy*, 2021.

[53] J. Reichel, F. Peck, M. Inaba, B. Moges, B. S. Chawla, and M. Chetty, “‘I have too much respect for my elders’: Understanding South African Mobile Users’ Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp,” in *Security 2020: USENIX Security Symposium*, 2020.

[54] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, “Investigating the Computer Security Practices and Needs of Journalists,” in *Security 2015: USENIX Security Symposium*, 2015.

[55] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub, “Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants,” in *CHI 2018: ACM Conference on Human Factors in Computing Systems*, 2018.

[56] C. Chen, N. Dell, and F. Roesner, “Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors,” in *Security 2019: USENIX Security Symposium*, 2019.

[57] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno, “Computer Security and Privacy for Refugees in the United States,” in *S&P 2018: IEEE Symposium on Security and Privacy*, 2018.

[58] M. J. Boyd, J. L. Sullivan Jr., M. Chetty, and B. Ur, “Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters,” in *CHI 2021: ACM Conference on Human Factors in Computing Systems*, 2021.

[59] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak, “ ‘No Telling Passcodes Out Because They’re Private’: Understanding Children’s Mental Models of Privacy and Security Online,” in *CHI 2017: ACM Conference on Human Factors in Computing Systems*, 2017.

[60] P. Kumar, J. Vitak, M. Chetty, T. L. Clegg, J. Yang, B. McNally, and E. Bonsignore, “Co-Designing Online Privacy-Related Games and Stories with Children,” in *CHI 2018: ACM Conference on Human Factors in Computing Systems*, 2018.

[61] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, “Why Older Adults (Don’t) Use Password Managers,” in *Security 2021: USENIX Security Symposium*, 2021.

[62] A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, “Privacy and Security Threat Models and Mitigation Strategies of Older Adults,” in *SOUPS 2019: Symposium on Usable Privacy and Security*, 2019.

[63] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, ““Warn Them” or “Just Block Them”?: Comparing Privacy Concerns of Older and Working Age Adults,” in *PETS 2021: Privacy Enhancing Technologies*, 2021.

[64] S. Murthy, K. S. Bhat, S. Das, and N. Kumar, “Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults,” in *CHI 2021: ACM Conference on Human Factors in Computing Systems*, 2021.

[65] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, ““Woe is me:” Examining Older Adults’ Perceptions of Privacy,” in *CHI EA 2019: Extended Abstracts of ACM Conference on Human Factors in Computing Systems*, 2019.

[66] T. Mendel, “Social Help: Developing Methods to Support Older Adults in Mobile Privacy and Security,” in *UbiComp/ISWC 2019: ACM International Joint Conference on Pervasive and Ubiquitous Computing and ACM International Symposium on Wearable Computers*, 2019.

[67] H. M. Mentis, G. Madjaroff, and A. K. Massey, “Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment,” in *CHI 2019: ACM Conference on Human Factors in Computing Systems*, 2019.

[68] A. McDonald, C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles, ““It’s stressful having all these phones”: Investigating Sex Workers’ Safety Goals, Risks, and Practices Online,” in *Security 2021: USENIX Security Symposium*, 2021.

[69] C. Barwulor, A. McDonald, E. Hargittai, and E. M. Redmiles, ““Disadvantaged in the American-Dominated Internet”: Sex, Work, and Technology,” in *CHI 2021: ACM Conference on Human Factors in Computing Systems*, 2021.

[70] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. S. Gaytán-Lugo, T. Matthews, S. Consolvo, and E. Churchill, “‘Privacy is not for me, it’s for those rich women”: Performative Privacy Practices on Mobile Phones by Women in South Asia,” in *SOUPS 2018: Symposium on Usable Privacy and Security*, 2018.

[71] B. Reaves, N. Scaife, A. Bates, P. Traynor, and K. R. Butler, “Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World,” in *Security 2015: USENIX Security Symposium*, 2015.

APPENDIX

A. Interview Protocol

Informed Consent

Thank you for meeting with me. My name is Collins and I am a student at the George Washington University. I am doing a study on mobile loan applications in Kenya. Before we begin, I am about to send you a document that informs you of the study procedure. You should read that document carefully, and please let me know if you have any questions.

If participant consents to take part in the study:

1) What mobile loan applications do you currently use and/or have used in the past?

For the next set of questions, I would like you to think about the mobile loan application you have most commonly used or use and answer these questions with that application in mind.

2) What mobile loan app have you most commonly used?
3) Please describe how this application works.
   Ask below follow-up questions if they are not addressed.
   a) How does it calculate your credit worthiness?
   b) What happens if you’re unable to pay back the loan?
4) Why do you use this mobile loan application?
5) What do you like the most about this mobile loan app?
6) What do you dislike the most about this mobile loan app?
7) Do you have any concerns with this mobile loan app?
   Ask below follow-up question if it is not mentioned.
   a) Any security and privacy concerns?
8) Have you stopped using any mobile loan application?
   Ask below follow-up questions if they are not addressed.
   a) What loan application?
   b) Why did you stop using it?

9) Have you removed any mobile loan app after using it?
Ask below follow-up questions if they are not addressed.
   a) What loan application?
   b) Why did you remove it?
10) All mobile applications require access to different permissions in order to access data required for one function or another. Mobile loan applications similarly require access to different permissions. What are the permissions required by the mobile loan application you have most commonly used or use?
Guide participants through the process if they are unfamiliar with it.
   a) What do you think this loan application does with these permissions? *Ensure participants provide an answer for all the permissions.*
   b) How did you learn about this?
   c) Are you comfortable with this?
11) What permissions requested by mobile loan apps, if any, are you least concerned about?
12) What permissions requested by mobile loan apps, if any, are you most concerned about?
13) Is there anything else you would like to share about mobile loan apps?
14) As a result of this interview, is there anything you will do differently with mobile loan applications going forward?

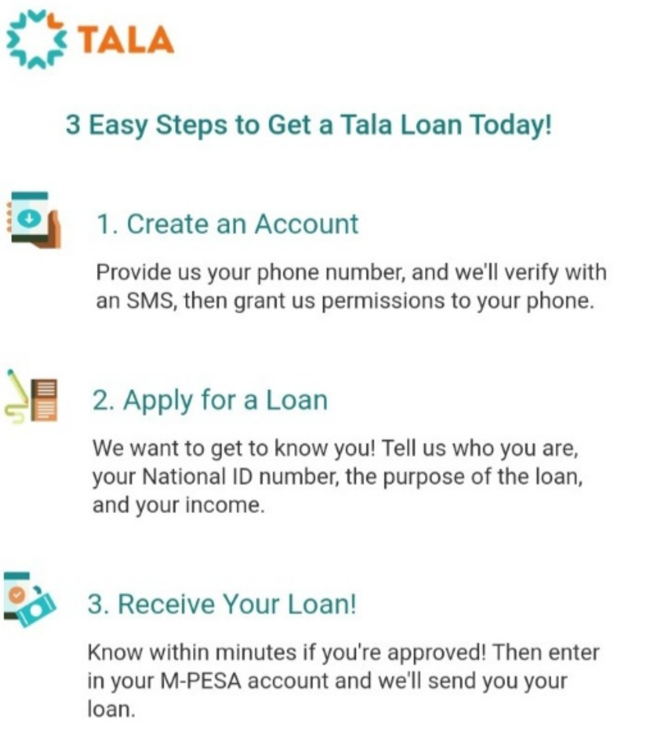
Demographics
Finally, I am going to ask you some demographic questions. If you prefer not to answer any of them, please let me know.

16) What is your age?
17) With which gender do you most identify with?
18) What is the highest degree or level of education you have attained?
19) Which of the following best describes your educational background or job field?
   - I have an education in, or work in, the field of computer science, computer engineering or IT.
   - I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT.
   - Prefer not to say.
20) How do you earn your living?
21) As an appreciation for your time, I would like to gift you 2GB of data or 125 minutes of call time to your phone. Which one do you prefer?
As per preference, the voucher is transferred to the participant's phone.

B. Qualitative Codes

- **mobile-loan-apps (64)**
Tala (14), Branch (13), OKash (8), OPesa (5), Zenka (5), Zash (2), LCash (2), MoKash (2), iCash (2), Timiza (2), iPesa (2), MyKES (1), Scoppe (1), Berry (1), CashNow (1), CreditHela (1), LionCash (1), CashApp (1)
- **loan-app-permissions (129)**
contacts (20), SMS (20), telephone (20), location (19), storage(19), camera (16), calendar (10), microphone (5)
- **permissions-use (140)**
SMS (26): *check-transactions (10), send-you-SMS-reminders (5), know-frequent-contacts (4), check-loan-defaults (2), phone-verification (2), text-contacts (1), send-you-updates (1), send-you-promotional-texts (1)*
contacts (22): *call/SMS-them-upon-defaulting (17), access/confirm-guarantors (3), call-you (2)*
location (22): *track-you (14), confirm-location (5), don't-know (2), customize-services (1)*
telephone (19): *don't-know (5), reminder-calls (3), send-you-money (3), track-you (2), confirm-phone-ownership (2), promotional-calls (1), call-contacts (1), check-phone-type (1), check-frequent-contacts (1)*
camera (18): *don't-know (7), take/upload-photo (6), assess-you/looks (3), track-you (1), spy-on-you (1)*
storage (18): *don't-know (12), app-installation (3), access-files (1), install-backdoor (1), check-other-apps (1)*
calendar (10): *know-pay-day (5), record-keeping (2), know-borrowing-date (1), locate-you (1), don't-know (1)*
microphone (5): *don't-know (2), talk-to-agent (2), record-you (1)*
- **loan-app-positives (38)**
quick-loan-disbursement (14), growing-borrowing-limits (7), no-paperwork/formalities-required (6), easy-access-to-loans (3), promotions/offers (2), small-interest-rates (2), MPesa-intergration (1), apps-have-reminders-to-pay (1), apps-don't-need-lending-reason (1), adequate-loan-amounts (1)
- **credit-worth-calculation (24)**
trust (5), check-transactions (4), don't-know (4), employment-details (4), check-CRB (3), data-from-permissions (2), social-media-data (1), telecoms-company-data (1)
- **loan-app-concerns (67)**
frequent-calls/SMS (13), borrowing-addiction (13), high-interest-rate (10), short-repayment-period (6), growing-interest (6), CRB-listing (4), data-shared-with-third-parties (4), penalties-for-delayed-payment (3), interest-deducted-upfront (2), no-option-to-delete-info (1), don't-know-data-handling (1), app-records-passwords (1), social-media-shaming (1), small-loan-amounts (1), other-people-borrowing (1)
- **concerning-permissions (35)**
contacts (24): *contacts-not-involved-in-loan (9), contacts-will-be-threatened (5), name-defamation (5), apps-should-stick-to-guarantors (4), contacts-will-be-tracked (1)*
camera (5): *spy-on-you (3), don't-know-use (2)*
SMS (2): *read-private-messages (2)*
location (2): *track-you (2)*
storage (2): *don't-know-use (1), app-will-misuse (1)*
- **non-concerning-permissions (26)**
storage (6): *don't-know-use (5), required-for-app-installation (1)*
location (6): *can-easily-move (3), required/already-provided (3)*
camera (4): *don't-know-use (2), take/upload-photo (1), immediately-remove-app-after-use (1)*
telephone (3): *don't-know-use (2), app-already-has-access (1)*
calendar (2): *don't-know-use (2), calendar-empty (1)*
contacts (2): *verify-guarantor (1), publicly-available (1)*
SMS (2): *no-private-SMS (1), comfortable-receiving-texts-from-app (1)*
- **loan-privacy-tradeoff (10)**
disregard-privacy-to-get-loan (10)
- **post-interview-behaviour (10)**
avoid/won't-use-loan-apps (6), check-permissions-before-use (3), minimize-usage (1)
- **additional-information (4)**
regulate-loan-apps (4)

C. Additional Figures


TALA

3 Easy Steps to Get a Tala Loan Today!

1. Create an Account

Provide us your phone number, and we'll verify with an SMS, then grant us permissions to your phone.

2. Apply for a Loan

We want to get to know you! Tell us who you are, your National ID number, the purpose of the loan, and your income.

3. Receive Your Loan!

Know within minutes if you're approved! Then enter in your M-PESA account and we'll send you your loan.

Fig. 3: Tala Loan Procurement Process.