‘I have too much respect for my elders’: Understanding South African Mobile Users’ Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp

Jake Reichel
Princeton University

Fleming Peck
Princeton University

Mikako Inaba
Princeton University

Bisrat Moges
Princeton University

Brahmnoor Singh Chawla
Princeton University

Marshini Chetty
University of Chicago

Abstract

Facebook usage is growing in developing countries, but we know little about how to tailor social media privacy settings to users in less well-resourced settings. To that end, we present findings from interviews of 52 current mobile social media users in South Africa. We found users’ primary privacy-related concern was who else could see their posts and messages, not what data the platforms or advertisers collect about them. Second, users displayed general knowledge gaps on existing social media privacy settings and relied heavily on blocking and passwords for privacy and security protection. Third, users’ privacy and security-related behaviors were heavily influenced by living in high-crime areas. Based on these findings, we suggest future work to better serve users’ privacy and security needs in less well-resourced settings.

1 Introduction

There are an estimated 139 million Facebook users in Africa and the most popular messaging app on the African continent is WhatsApp, also owned by Facebook [34, 50, 58]. Most of these users are on mobile only and may be unaware of privacy issues [22, 34], thus making them more vulnerable to exploitation of their data [53, 69]. Yet most of the research on how users manage privacy on Facebook has been undertaken in more well resourced countries and has not focused on low income users specifically [10, 63]. This is significant, since in developing contexts in many African countries, many other factors such as costly data plans, issues of device ownership and phone sharing, and differences in culture influence social media users’ privacy [44, 48, 68, 69]. Several researchers have been investigating social media usage in Ghana, Kenya, India, parts of South Asia, parts of the Arab gulf, and South Africa including Facebook and Free Basics usage, the zero-rated platform for applications—meaning users do not have to pay for data costs for using these applications—made by Facebook [3, 53, 56, 57, 75–78]. Although these studies focus on low income users, fewer focus specifically on how users manage their privacy on these social media applications. Given the fact that privacy is a very culturally bound concept [5, 15, 68, 69] and to avoid over-generalizing from one marginalized community to another, it is important to understand how users in South Africa approach the management of privacy and privacy settings on Facebook and its related applications [44]. Moreover, the ‘privacy paradox’ suggests users’ privacy concerns may not be correlated with actual privacy protecting behaviors; thus, studying current social media behaviors which are better correlated with users’ privacy valuations is crucial [8, 12, 52]. Doing so can help inform the design of privacy settings for users whose needs may not have been accounted for [67].

To investigate how resource-constrained mobile users perceive and manage their privacy on social media, we conducted a qualitative study with 52 mobile social media users in Cape Town, South Africa. We focused our study on the Facebook suite of apps—Facebook, WhatsApp, Instagram, and Free Basics, (a platform for applications including Facebook Lite, Messenger Lite, and others)—since they are the most popular apps in South Africa, particularly amongst low income users [53]. Our goals were to better understand users’ mental models of privacy, what data privacy options are available to them, and their social media consumption patterns. We also aimed to develop recommendations for improving privacy and potentially security controls for these users specifically. We had three research questions: (1)What are South African mobile social media users’ privacy concerns?, (2) How do users currently manage privacy on social media?, and (3) What factors influence users’ current behaviors on social media?.

We have three main findings. First, we found that users’ principal privacy concerns regarded who had access to information they considered private as opposed to platforms collecting data about them. In particular, users were mindful of *‘elders’* and others and how they presented themselves online. Users also perceived WhatsApp as more private than Facebook because they understood the settings and felt the audience on the platform was more under their control. Second, much like in more well resourced settings [68], we found that users had very little knowledge of available privacy settings or how to use them. Unlike in more developed settings,

their primary method of protecting privacy was via blocking people or controlling what they posted or via passwords on shared devices, as opposed to relying on granular privacy settings [15]. Third, unlike more developed settings, we found evidence that users' concerns for physical safety strongly impacted when and what they posted on social media. High crime, phone sharing, and theft also influenced account hacking, what content they encountered, and how they used social media to store their data. Based on these findings, we make recommendations to better address the privacy and security needs of mobile users in high-crime settings.

We make two contributions. The first is providing evidence of how low income users in South Africa manage privacy on Facebook and WhatsApp, which adds to a growing set of literature on privacy behaviors on social media in other low-income countries and regions including Ghana, parts of South Asia, Saudi Arabia, and parts of the Arab Gulf [3, 13, 51, 57]. This evidence provides novel insights about how cultural and financial differences affect privacy management in marginalized communities and how South African concerns compare to those of users in various resource-constrained nations. The second contribution is providing recommendations for how to address user needs for privacy management in marginalized communities in high-crime settings, again building on unique insights from South Africa, such as data costs limiting users' explorations of privacy settings, and user concerns around physical safety affecting posting on social media. In the rest of this paper: Section 2 explores prior work, Section 3 and 4 detail the methods used and our findings. Finally, Section 5 discusses the implications of our findings for marginalized users' social media privacy needs[1].

2 Related Work

2.1 Social Media And Privacy Breaches

With the rise of social media usage, social media companies have found new ways to monetize their users' data [25], including by encroaching on user privacy with methods ranging from allowing third-party app access to user information to massive data collection by the platforms themselves [20, 30, 71]. This "Big Data" era has brought along with it a renewed emphasis on data privacy. Facebook has been in the spotlight a number of times recently for major data breaches and how it treats user privacy. For instance, in 2018, after a major backlash from users about data breaches at Facebook through Cambridge Analytica, Facebook executives Sheryl Sandberg and Mark Zuckerberg testified in front of the United States Congress about the use of data in targeted advertising during the 2016 United States presidential election [62]. Even after such testimony, many calls for social media sites to improve the way they handle user data remain unanswered.

[1]There are currently no guidelines for respectful writing on resource-constrained settings but we strived to present our work respectfully drawing inspiration from http://interactions.acm.org/archive/view/november-december-2015/writing-about-accessibility.

In late December 2018, a *New York Times* exposé [17] revealed that Facebook had been giving other major companies, such as Microsoft, Amazon, and Spotify, access to private messages sent through Facebook's Messenger application. Other social media sites have also been at the helm of controversy over privacy breaches. For instance, a few weeks after the Facebook Messenger app story broke, a massive security flaw in Google's social media site, Google+, was reported to have exposed the data of more than 52 million users [45]. A *Wall Street Journal* investigation later showed that Google had known about this bug for more than three years, but feared the repercussions of revealing it to the public [39]. Despite media attention, discussion regarding these events has not been about protecting the end users themselves, but rather, has been largely surrounding the notion that technology conglomerates have grown too powerful by using consumer data.

Additionally, it is increasingly evident that social media users are not even aware of the vast data collection done by companies. A study [29] conducted by the Pew Research Center found that only 12% of adult Facebook users were aware that Facebook maintained a list of their interests and identifiable traits. Once informed, however, 82% expressed at least some level of unease about a company collecting this information about them. Further, researchers found [6] that the mechanisms Facebook currently uses to inform users about data collection in an effort for transparency, such as the "ad preference" page and the "why am I seeing this?" button, give users misleading or erroneous explanations about the data Facebook has collected about them. Thus, users often lack knowledge about data privacy practices on social media.

2.2 Facebook And Privacy Studies

Ironically, while stories about breaches of digital privacy continue to populate daily news outlets and an increasing number of countries are passing laws protecting user data privacy [26], researchers have found that the users in developed countries have not been taking many measures to protect their data. Users continue to post and upload large amounts of personal information, despite claiming high levels of knowledge of privacy issues [19, 65]. Users do, however, use various strategies such as self-censorship and information control to manage their privacy as found by Cho and Filippova who studied hundreds of users in the United States and Singapore to see how they manage privacy on Facebook [14, 15]. Some studies also focus on how users perceive data collection and privacy from third-party apps on Facebook [35, 72]. Notably, most existing studies of Facebook and privacy have been conducted in developed countries such as the United States [9, 31, 37, 61, 73], and Canada [79]. Additionally, many studies relied only on student populations. Thus this vast literature is not necessarily representative of users privacy behaviors in developing countries who may be mobile only, experience high data costs, or engage in phone sharing [4, 40, 53].

However, there is a growing amount of research on how

users in developing countries use social media platforms. Some studies have focused broadly on Internet use, such as in Bangladesh [11] and Havana [21], or the use of voice social media platforms for blind users in India. These studies have confirmed that users in less-resourced settings use social media platforms such as Facebook, Twitter, and WhatsApp, often by consuming content more so than posting. Yet, these studies have not not focused on how users manage privacy on these platforms specifically. Others focus on privacy attitudes and privacy on mobile phones in India and other countries in South Asia or on how social media users experience online abuse, without specific focus on privacy management [36, 56, 57, 70].

2.2.1 Social Media Use and Non-Use

There are also studies specifically on social media usage and non-use. For instance, Miller conducted a year-long study of Facebook in Trinidad [43]. In another study, Wyche et. al [77] found that in a low-income neighborhood in Nairobi, Kenya, Facebook was mostly used for purposes of income generation and supplementation such as looking for job opportunities or marketing oneself. A different study done in Kenya by the same researchers [78] found that usage of Facebook was desired, but limited. Low income users' minimal Facebook use often took place at Internet cafes, as participants either did not have the financial resources to spend money on mobile data plans or encountered infrastructural challenges such as power outages, low-bandwidth, and limited Internet connectivity. In a third study by Wyche [75] in a Nairobi slum, she found that often women were harassed online on Facebook. All of these studies were done in Kenya. Some researchers also studied urban users' [13] perception of online security threats in Ghana. They found that at least 26% of 193 respondents reported using at least one Facebook privacy setting.

2.2.2 Privacy and Social Media In Marginalized Communities

A few studies do explore privacy behaviors on social media in detail in non-African countries. This prior work suggests users do make use of granular privacy settings to limit personal information being shared widely. One study of Saudi Arabian WhatsApp users' privacy behaviors [51] found that more than half the users had used a WhatsApp privacy setting and tried to hide their "Last Seen" feature on WhatsApp (showing when a user was last online). In another study of social media privacy in the Arab gulf [3], the researchers found that users often had private Facebook accounts or used post-level privacy settings to avoid bringing dishonor to their families through exposing personal information that was not in line with their culture or religious beliefs. Females, in particular, struggled from unwanted contact and scrutiny on social media. These studies shed light on privacy behaviors in various marginalized communities, but it is unclear how these takeaways apply to the South African context.

The study most closely related to ours examined how aware South African college students at NorthWest University were of South African online privacy-related legislation, such as the Protection of Private Information Act [47]. In this survey-based study, Nyoni and Velempini found that users did not take advantage of many privacy features when accessing their Facebook profiles. They discovered that 86% of respondents were "not aware of the [settings or] controls that can assist them to regulate their privacy," such as being able to set who is permitted to tag them in a picture, post on their wall, or prevent their location from being shared. Further, the researchers found [46] that 81% of those surveyed indicated that they were unaware of the rights granted to them by South African legislation. This study suggests that South African social media users follow the global trend of lack of knowledge of privacy law or practices [64].

That study had a limited focus on Facebook usage only, and all participants were selected from individuals who had "liked" the NorthWest University Facebook page. Our study, by contrast, gathered data from a diverse participant pool across a city. Furthermore, we examined Facebook privacy management as well as its related applications. Our study adds to this growing body of work by focusing on how low-income South African mobile users manage privacy on Facebook and related applications WhatsApp, Instagram, and Free Basics through in-depth interviews with current and active users.

3 Study Method And Participants

To answer our research questions, the first author and a local research assistant conducted 52 in-person interviews with mobile social media users in Cape Town, South Africa between November 2018 and February 2019. The study was approved by Princeton's Institutional Review Board (IRB).

3.1 South African Research Context

In South Africa, there are approximately 18 million social media users, 89% of whom browse social media exclusively from their mobile devices [59]. An earlier study found that these users are often resource-constrained, as data costs are extremely expensive [40]. Additionally, the study found that many low-income users are commonly on prepaid plans, using up a large portion of their income on Internet use. Thus, many users have turned to using zero-rated versions of applications such as Facebook's Free Basics platform. However, a study done in 2018 [53] found that Free Basics users in South Africa are unknowingly agreeing to additional data tracking in exchange for free data, meaning that these users are left more exposed in terms of privacy from the provider than users of paid versions of those applications.[2] Moreover, a study on global Internet usage found that African countries tend to rank near the bottom of all countries in terms of Internet connection speeds, which also slows down social media usage [34].

[2]Free Basics uses a proxy for all apps offered through the platform allowing Facebook access to data from all apps. This is not the case if a user is using a paid version of the same app.

3.2 Recruitment

We recruited participants over the age of 18 who lived and worked in South Africa. We filtered for participants with personal smart phones who were current users of the following social media applications: Facebook, WhatsApp, Instagram, and Facebook's Free Basics platform. Users had to report using at least one of these apps for at least three hours a day to filter out novice users. This step ensured our users were consistent with the profile of an average African user who typically spends about three hours daily on social media [55]. We focused on these applications because Facebook is the most popular social media application in South Africa according to Alexa's rankings [1] and these other applications are part of the Facebook suite. In addition, WhatsApp is one of the most popular messaging applications in South Africa [60].

We recruited individuals through a variety of means, with the understanding that users in different socioeconomic circumstances may have different usage patterns. To attract middle to upper class users, we created a targeted Facebook advertisement for users who were between the ages of 18 and 65, lived within 10 miles of Cape Town, and primarily accessed Facebook from mobile devices. At the same time, we created a banner advertisement on MyBroadband, South Africa's largest IT news site (ranked 60 on Alexa SA rankings [1]). On both of those platforms, users who clicked on the advertisement were directed to fill out a questionnaire to ensure that they were eligible for the study. We also publicized the study on our research website and on Twitter.

To recruit individuals from lower-income backgrounds, our research assistant in South Africa went into "spaza" shops (small convenience stores) within the lower income communities of Langa, Delft, and Khayelitsha [18] which all form part of a violence-prone area of Cape Town known as the Cape Flats [2]. Individuals who were buying airtime were approached and asked if they would agree to participate in our study. Upon confirming their eligibility, our research assistant would set an appointment with them. Often, these individuals would refer others for participation, but close friends or family were not interviewed, so as not to bias the data.

None of our recruitment texts or verbal methods made any reference to "security" or "privacy" to ensure that we were not priming the subjects; rather, participants were told they would be having a general conversation about "usage of social media applications." We received interest from 54 individuals through the online advertisements. Of those, we were able to schedule interviews with 16, due to time and availability constraints, of which 12 arrived at their arranged times to complete their respective interviews. Additionally, of the 41 individuals recruited from lower-income communities, 40 completed their interviews, bringing the total number of participants to 52. Attempts to remotely interview remaining respondents on Skype were unsuccessful.

3.3 Interviews

Before participating in any interviews, each participant had to complete two surveys. First, each completed a questionnaire that asked them how long they had been using social media and which social media applications they used most frequently of Facebook, WhatsApp, Instagram, and Free Basics. We also asked if they used Snapchat, Twitter, or YouTube. Secondly, each participant was given a demographic survey to complete or verbally completed a survey that asked them for their race/ethnicity, age, and gender identity.

Once participants completed the surveys, they were invited for interviews. Those who had the means to travel were interviewed at a non-profit organization headquartered in Cape Town and three were interviewed on Skype. All participants from the Cape Flats were interviewed in their homes or home-like settings near their places of residence. Additionally, all interviews in the Cape Flats region were strictly time-bounded, because the area is generally unsafe, and we did not want our female research assistant to spend any more time than absolutely necessary in the area. In some cases, this meant we could not probe deeper into all topics e.g., detailed privacy setting use on each social media application mentioned.

Most interviews were conducted in Xhosa (30/52), an official language of South Africa and the remainder were conducted in English. All interviewees signed consent forms before their interviews, which were all audio-recorded. Each interview lasted approximately thirty to forty-five minutes and participants were compensated for their participation with a ZAR300 ($21 USD) gift voucher to `Takealot.com`, a widely-used online shopping website in South Africa.

Each interview followed a tiered structure of questioning to better understand participant's mental models of privacy and how they manage privacy on the Facebook suite of applications. First, the participants were asked questions about their phones and their mobile data plans. Next, they were asked about their usage on the applications: which of these social media applications they visited most often and what their general usage patterns were on each of those applications. We did not ask about social media usage in a mobile browser. We then asked the participants questions relating to their privacy behaviors: who they thought could see their posts, which applications they were willing to share more information on, what information they thought companies collect about them, and if they knew of any settings on their social media applications that could help them maintain their online privacy. Lastly, we asked participants questions relating to their online privacy behavior: how they maintain their privacy on the Internet, what tools, if any, they use to ensure their privacy, if they had ever experienced a breach of privacy, and about their usage of privacy settings on the Facebook suite of applications or other applications/tool used for privacy purposes.

Example questions asked included:'Is there anything you avoid doing on social media? What? Why?', 'What does pri-

Age			**Ethnicity**			**Household Annual Income in USD**			**Gender**	
Group	*Total*		*Group*	*Total*		*Group*	*Total*		*Group*	*Total*
18-25	24		Black	46		Very Low Income (0−1,444)	25		Male	22
26-34	15		White	5		Low Income (1,445−6,530)	11		Female	29
35-44	10		Indian/Asian	1		Low Emerging Middle Class (6,531−14,482)	3		Non-binary	1
45-54	2					Entering Middle Class (14,483−29,570)	4			
55+	1					Did Not Disclose	9			

Table 1: Demographic breakdown of participants. Income is reported in United States Dollars (USD)

vacy on the Internet mean to you?' and 'Are you aware of privacy settings in any of the social media applications you use?'. While the interviewers had a prepared set of questions to ask the participants, all interviews followed a semi-structured format, so the researcher would follow up on particular questions or subjects that generated unanticipated or relevant feedback from each participant, which tended to vary vastly based on the user's usage patterns. All interviews were audio-taped.

3.4 Analysis

We first transcribed the audio files, translating the 30 interviews that were conducted in Xhosa to English, and then performed qualitative data coding on the transcripts. During this process we tagged similar phrases or sentiments shared by the participants using structural coding and thematic analysis [54]. The initial codebook we created was, at first, largely based on the interview guide, and was shared with our team of five coders. Additionally, we edited and enhanced the codebook as we noticed trends emerging from our first pass over the interviews. There were a total of 17 parent codes, with each of them having 2-4 child codes, for a total of 34 codes as shown in the Appendix. Examples of parent codes included: 'Activities on phone' and 'Crime' and example of child codes included: 'Expressed concern over advertisements' and 'Usage of privacy settings'.

Each interview underwent two rounds of coding by the research team, comprised of 5 undergraduate students, including the lead author, all trained in qualitative analysis. Each transcript was coded by the lead author and at least one of the other coders, and was reviewed by the most senior author. Once all the files were coded, each coder was assigned 1-2 parent codes and provided with all interview excerpts tagged with those codes. Each coder performed a thematic analysis on these excerpts and wrote a thematic summary. The research team then held regular meetings to review all of the summaries and to decide on the final themes that are discussed in the paper. Owing to the coding process, we did not calculate inter-rater reliability (IRR) because thematic analysis does not lend itself to such calculations and shared consensus can still be reached without this measure [7]. [3]

[3] As per McDonald et al. [41], calculating IRR is not necessary because our coded data was not our end-goal but used as input for thematic analysis. Although we did use multiple coders, all of our transcripts were read by the lead and senior authors to ensure consistency. We resolved disagreements using a dedicated Slack channel, email, and regular in-person team meetings.

In all interview snippets in this paper, *I* means that the interviewer is speaking. Participants P1 through P12 were interviewed by the first author in downtown Cape Town, while participants P13 through P52 were from the Cape Flats and interviewed by our South African research assistant.

3.5 Participants

Our participants were very diverse (Table 1) with a nearly even representation of females and males in the study. The interviewees tended to skew towards a younger age range, consistent with what should be expected for social media usage in South Africa [16]. Additionally, we asked individuals what their household income levels were, so that we could better understand if income levels had an influence on privacy mental models. Using the Momentum Unisa Financial Wellness Index [66] as a reference, we confirmed that most of the participants fell into a lower-income bracket.

The majority of the participants were under 35 years of age and most were Black with the remaining being White or Indian/Asian. 10/52 participants were students and 23/52 were unemployed. Of those participants who disclosed income, the majority earned less than ZAR21,500 ($1,444 USD) annually. In the past 6 months, 24/52 participants reported that they were unable to afford groceries in the last month, 26/52 reported that they were concerned about paying bills, and 3/52 reported that their utilities were shut off due to unpaid bills. 90% of the Cape Flats participants reported being dependent on welfare with no other source of income.

All of the participants reported using WhatsApp; only four fewer reported Facebook use (Table 2). Fewer than half reported using Instagram. More than a third of participants used at least one of these three applications for greater than five hours a day, while 23 others reported daily usage of between three and five hours. Fewer participants used YouTube and Snapchat, thus discussion of those apps was much more limited. The amount of time they had been using social media varied. Many of the low income participants mentioned that they often did not use apps that used up a lot of data such as Instagram; they tried to use free apps and promotions such as when one of the cellular networks offered Twitter for free and Facebook's Free Basics platform. Similar to findings in poor areas of Kenya [75, 77, 78], participants said that they use their phones for social media and to search for jobs.

Category	Subcategory	Count (X/52)	Percent
App Use			
	WhatsApp	52	100%
	Facebook	48	92%
	YouTube	19	37%
	Instagram	16	31%
	Snapchat	5	10%
Daily Use			
	>5 hours	21	40%
	4-5 hours	23	45%
	$\leq$ 3 hours	8	15%
Lifetime Use			
	>7 years	23	44%
	4-7 years	16	31%
	<4 years	13	23%

Table 2: Breakdown of participant social media habits

For the majority of participants in our study, WhatsApp was their primary application used for messaging, whereas Facebook was used more as a general social networking platform. Participants also told us that WhatsApp was also preferred because it uses far less data than Facebook, making it more accessible and less expensive to use. Similarly, the few participants who mentioned other social media apps, often spoke of using these apps such as Twitter when there was a free promotion to use it on their service provider or on a friend's phone or an Internet cafe. In a population in which data is more of a luxury [53], ease of access is of high consideration[4].

4 Findings

The main themes that emerged from the interviews were as follows: First, the participants' privacy concerns were primarily centered around controlling their information and around who would be able to see their posts and messages. Second, participants displayed a major lack of knowledge of available privacy settings on the suite of Facebook social media applications and relied heavily on blocking as a privacy protection measure or passwords on apps and phones. Third, for users in lower-income, high-crime settings such as South Africa, physical safety heavily influences their conceptions of, and posting behaviors on social media. Notably, we did not find any strong contrasts in privacy *concerns* between lower and middle income participants in our study, with two exceptions: Firstly, only the lower-income individuals discussed using Facebook as a data storage platform (4.3.4). Secondly, a few of the middle-to-upper income individuals were well-versed in online privacy matters; but, they were recruited through an online broadband forum and research social networks which could account for a more technically savvy sample. One or two of these participants were aware of online tracking by social media platforms but this was not mentioned by any low and middle income participants. Lastly, the lack of a strong distinction between the two groups may be due to having fewer middle-to-upper income participants overall.

4.1 Users Privacy Perceptions

When participants were asked about their privacy on social media, the majority spoke from the perspective of "who will be able to see what I am doing on social media?". The notion of privacy from a service provider was not commonly raised nor was there a concern about data collection for advertising purposes; instead, participants were focused on privacy from other people. Some (6) even went as far as to say WhatsApp does not collect information on their users at all. Most participants instead expressed concerns about known contacts seeing undesirable content or whether their significant other would be able to access participants' private content on their phones and social media accounts. These privacy concerns echo those of shared mobile phone users in low income countries such as Bangladesh [4]. Out of the group of users (11/52) who did mention that online tracking could be an issue or that companies have a motive to do so, only two mentioned data collection for advertising purposes.

4.1.1 Privacy Perceived As Information Control

The majority of our participants defined privacy on the Internet as selectively sharing information online to regulate who could have access to posts. That is, users in our study primarily talked about privacy as *'information control'* [14, 15].

> P18: When we speak of privacy, I think of something that is secret information that one keeps to themselves. When it comes to the Internet or social media, sharing something with someone in [private] means you don't want it to be seen by other people.

Some participants mentioned privacy, but when they discussed it further they also included talk about security issues, such as preventing hacking and securing information. For instance, many participants spoke of their Facebook accounts being compromised by friends or others stealing their passwords and posting content they felt was inappropriate or not reflective of themselves.

> P31: There's no privacy on the Internet because there are hackers out there. Even if I think no one can see my messages, there is someone that can see them. I've been hacked once and the person who hacked my Facebook account sent a message to my cousin saying "I'm tired of being straight now and hiding myself. I'm going to be gay now." and they sent it using my account. I don't know this person and I even tried to stop this by changing my password, so that's why I'm saying there's no

[4]The zero-rated version of Messenger, Messenger Lite, has been available for most Android users since 2017. It has yet to be released for iOS across the world [49]. For an in depth study of Facebook's Free Basics platform, see Romanosky and Chetty, 2018.

privacy on the Internet— since I was hacked before.

In other cases, participants talked about privacy being important as it could impact physical safety. For instance, one participant mentioned the *stokvel* to which they belonged; essentially an informal credit union where 10 to 12 members contribute money that is divided on a fortnightly basis to members [42].[5]. This theme of privacy being tied to high crime was recurring amongst participants.

> P38: Yes it's important because, if we want to meet, maybe someone who knows us sees our conversation. Say maybe a stokvel is dividing the monies on a certain day, and the person might organize for people to come rob us of the monies the stokvel is dividing to its members.

The remaining ten participants expressed an uncommon belief amongst the interviewees that there is no such thing as privacy on the Internet or on various social networks since they are intrinsically meant to share your information with other users. For instance, participants often felt that sharing more on Facebook could lead to finding jobs, lost friends or family, and being in contact with people in nearby suburbs, cities, or other provinces (such as *'Tokai'* (Cape Town), *'Johannesburg'*, *'Eastern Cape'*). Only a few participants had no conception of privacy at all (e.g., P52 defined privacy as *"Whoever created social media respects other people's views"*).

Interestingly, participants often conflated privacy with security given their definition of privacy as access control. For instance, many participants told us that *'privacy was extremely important'* to them and then proceeded to explain that their only method for protecting both online and offline access to their data was through the usage of a password. This is notable given reports of a security breach in which Facebook was storing hundreds of millions of passwords in plaintext, disproportionately affecting the users of their zero-rated platform Facebook Lite [74], commonly used by low-income communities such as those our participants lived in[6]. At least 13 participants described passwords as their only defense against privacy breaches, best illustrated by P33's definition of managing privacy on the Internet:

> P33: I think it means being safe from other people because they can use your profile picture to commit fraud and ruin your life, so I think that is where the settings come in.
> I: How do you keep your privacy on social media and make sure that it doesn't happen to you?
> P33: I keep my passwords to myself and I don't share them with anyone.

[5]Every month a different member gets the pot of money and this member rotates so that everybody has a turn to get the money.

[6]We were unable to discern when participants were discussing Facebook versus Facebook Lite on Free Basics. We can report that more than 20 of our participants used Facebook Lite at least some of the time.

4.1.2 Presentation of Self and Privacy from Elders

Participants expressed specific privacy concerns about how they presented themselves to others [23]. This concern about representing oneself to ones family members and relatives, and in particular, being respectful of, and maintaining privacy from *'elders'* was repeated by participants. Our participants often spoke of a worry that family members, friends, potential employers, or business partners would see inappropriate or less desirable content from them. For example, one individual, P35, was worried that his new girlfriend would be able to see the old pictures with his ex-girlfriend that he had posted on Facebook. He feared her seeing the *'wild life'* he had lived before. Similarly, P18 said that he stopped using Facebook after old pictures that he had posted on Facebook were *'stolen'* and then shared in a WhatsApp group to *'mock'* him. A significant portion of participants talked about hiding information from *'elders'*, people at *'church'*, their *'community'* or the *'village'* they had moved from to ensure they were not representing themselves in a bad light, because they felt judged. In one example, a female participant mentioned she worried about posting photos wearing tights because this was frowned upon for a *'married woman'*. In another case, P18 said:

> I have too much respect for my elders and I do not want them to see pictures of me and my boyfriend all over social media.

Participants told us that they tried to manage their privacy while still giving access to people that they felt could offer them opportunities such as jobs. A participant talking about this tension explained:

> P26: Parents, people that I usually work with. So I make sure that they don't see some stuff and also some family members who are my contacts on WhatsApp. So I make sure they don't see. More so the people who give me opportunities or people that I can benefit from are the ones that I make sure don't see some things.

In many cases, participants spoke of self-censoring their posts by editing photos, avoiding posting about *'personal issues'* or relationships or in some cases, posting or *'ranting'* about race which is a hot-button issue in South Africa to maintain their desired presentation of self. Only one or two of the middle income participants mentioned being concerned about posting photos with their *'ID number'* or identity number, the unique identifier for each citizen in the country.

4.1.3 WhatsApp Seen As More Private Than Facebook

Many participants highlighted what they valued in privacy settings by comparing WhatsApp and Facebook. Most of our participants tended to describe their level of privacy concerns in terms of how much they trust the people they interact with or how others behave on a particular social media platform as opposed to how much they trust the platform providers.

Participants told us that because more users have access to posted material on Facebook, they tended to trust Facebook less than WhatsApp. The number of people who have access to the conversations or statuses strongly impacted their perception of platform privacy. Participants felt that Facebook is a more public facing platform. For instance, one participant purposefully set his Facebook account settings to "public" so that long lost friends would be able to find him if necessary. The following quote illustrates this belief:

> P3: All the things one posts on Facebook are available for the whole world to see. I don't post things that I think will backfire on my image and name one day. Just the fact that everyone and anyone can see other people's posts makes me not trust the app.
> I: Are you in control of that? Are you able to decide who can see what you posted or not?
> P3: No, I am not in control. I think that even people I don't know can see my posts. I can post personal things on WhatsApp because I know the people who will see my status updates, whereas on Facebook, I am aware that even people I don't know can see all of my posts.

While the majority of users reported that they felt uncomfortable being added by users on Facebook whom they did not know personally, many of them added these individuals anyways. Often, participants did so because they felt that adding strangers might lead to new job opportunities or thought it would be *'rude not to add them.'*

Contrarily, participants explained that on WhatsApp, someone must have your number for them to access your content. This made participants feel that it is a more personal social media platform [32]. Because this is the default way of adding contacts, participants often had different types of relationships with their contacts on WhatsApp compared to their contacts on other platforms such as Facebook. Generally speaking, participants described that they used WhatsApp to communicate with close friends and family, describing it as *'private'*, and used Facebook to stay in touch with acquaintances.

> P24: Yeah. I think on Facebook, I'll add most people I know. With WhatsApp, it's more a personal thing, you know? People you chat with regularly.

The intimate nature of WhatsApp gave many users a sense of privacy because conversations can be between fewer people rather than a public post. Participants' praise of WhatsApp's privacy levels when discussing group messages on WhatsApp was much more reserved. For instance, participants mentioned that in group chats, they did not necessarily know every individual in the group chat, demonstrating that the *'intimacy'* factor influenced their conceptions of how private the platform is. Furthermore, on WhatsApp, participants described receiving more responses to their status messages, which causes them to post on WhatsApp more often. (A status message on WhatsApp is very similar to a *story* on Instagram or Facebook. It is an ephemeral posting, generally a picture or video, that will be visible to all of the person's contacts by default.) Participants commented on how more posts then lead to more status views by their friends. The high volume of responses on WhatsApp, similar to the one on one nature of the conversations, created a feeling of intimacy between a user and their contacts. Participant P21, who reporting using Instagram, Facebook, and WhatsApp regularly, said he feels a sense of privacy on WhatsApp because you can delete a message from both sides of the conversation, giving them control over what the other person in the conversation sees as well[7].

> P21: On WhatsApp you can actually restrict who can see your profile, and who you don't want to see it. And when you type and send something by accident, you can delete it on their side of the chat.

4.2 Current Privacy Behaviors

According to an earlier study done in Ghana, knowledge of privacy settings is hugely lacking, with only 25.9% of respondents reporting having used Facebook privacy settings before [13] — a nominal rate considering the extremely common usage of Facebook. Our participants reported similar usage rates for privacy settings. They often were unaware that privacy settings exist on social media and did not specific exactly which options they typically use in privacy settings, even if the topic came up.

4.2.1 Unaware Of Or How To Use Most Privacy Settings

In our study, at least 30 participants explicitly stated that they do not use or do not know how to use most privacy settings for their social media accounts. Also, unlike in similar settings [3], our participants had a far less nuanced understanding and use of other social media privacy settings such as changing who could see a post, creating lists of friends, changing who can see what is posted on a *'wall'*, who can see tagged photos, and so forth. Some participants did mention limiting their Facebook profiles to be seen by friends only and talked about public versus private posts but they were in the minority. At least one person mentioned 'unfriending' someone. Participants also felt a tension between wanting to be *'social'* and accessible to people who could give them opportunities and avoiding being too *'private'*. Nearly every time a participant expressed awareness of these privacy settings, they followed by explaining they had an inability to actually access the privacy settings, often mentioning data costs which we took to be the limiting factor. Earlier studies suggest users often follow their friend's privacy tendencies on Facebook [33]. Somewhat relatedly, in our study, we found that 11 participants who did know about privacy settings had often discovered these settings by either word of mouth or via a friend informing

[7] This feature was deployed on Messenger as well in February 2019 [28]

them of their existence or demonstrating how to use a particular control. These participants explained that they leveraged their friend's knowledge to prevent stalkers from seeing their profile and status on social media.

> P33: I would hear from my friends that you can go and follow these steps to achieve this private setting on your Facebook or WhatsApp to avoid being stalked on your social media. And I would listen and apply the advice.

Others wanted to prevent their family from seeing posts with them doing things not in line with their family's traditional values or that would be disrespectful to *'elders'*, but did not know how to do so until they were shown by friends.

> P29: My one cousin showed me, there is an option there that lets you choose who can see your status. I don't know how she does it. She is coming on Friday, I will ask her to show me again.

In fewer cases, participants found the settings on their own, such as P49, who spoke of altering settings to protect her privacy from elders:

> P49: Yes, because there are elders on my WhatsApp so I just rather not post or I hide the post. For example, if I take a picture somewhere and I am with my friends and there is alcohol in the shot. I learned this from just fiddling with my phone. No one told me about it.

Without knowing the settings, others resorted to opening a second or sometimes third Facebook account using different surnames, such as their mothers to limit who could see their content. One participant P24 talked about how she was on their third Facebook account because the first two had *'a lot of people I don't want'* that they didn't want to see their content anymore. Participants had different stances on the privacy settings of the two most frequently used social media applications: Facebook and WhatsApp. Our participants who knew about the many types of privacy settings that Facebook offers, such as making one's account private, tended to find it difficult to use them, even though they use those features on other social media sites. In multiple cases, when the interviewer demonstrated to the participant how to navigate to the privacy settings in the mobile application, the participant was surprised that such a page existed. It appeared that participants either did not spend the time required to find the privacy settings, or did not have the extra data to spend on navigating the nested pages on the application to find privacy settings. A few exceptions existed such as:

> P13: Well Facebook, I mean that depends on what your security settings is, and obviously each post, it can share to a certain audience. In WhatsApp, you can even set it there to [control] who can see your profile pic. So it's all about settings. A lot of people don't know about these settings.

More participants appeared to know how to configure their privacy settings on WhatsApp, such as being able to specify who can view a specific status message or chat, than did for other social media apps. Notably, participants did not mention limiting who could see WhatsApp's "Last Seen" feature.

> P41: Okay, WhatsApp you can hide as much as you can hide on the others, but you can hide who sees your stuff like your status, your personal life status, your profile picture. All of that! You can manage who sees all of that.

What became clear from the interviews is that many participants simply leave their privacy settings on the default, not knowing that they can even be changed. However, once users were told by their peers about varying levels of privacy control, they tried to change their settings to adjust their privacy accordingly, with data sometimes being the limiting factor. Participants who did know about such settings, found Facebook privacy settings more difficult to use than WhatsApp.

4.2.2 Blocking Used Instead Of Other Privacy Settings

Participants who were concerned with their privacy most frequently resorted to blocking people instead of using other privacy settings within the applications. In Saudi Arabia, WhatsApp users similarly used blocking to avoid unwanted contact from known and unknown contacts [51]. At least 17 participants talked about seeing inappropriate content or receiving harassing messages from people they did not know. Many participants mentioned that they received messages from strangers asking for meetings or for them to share nude photos or in some cases, pictures of genitalia from strangers. For instance, one participant mentioned getting messages from prisoners, another talked about getting messages from males that she did not know. These participants lamented not wanting this undesired contact from strangers but many did not know how to limit their settings to friends only.

> P14: Like in your inbox, other people add you on Facebook and inbox that they love you. They don't know you, they just saw you on Facebook and they calling you beautiful, trying to meet and call you. Such things irritate me. Other people send you pictures of their private parts or ask you to send pictures of yours, see things like that.

Most participants in our study more commonly reported using the blocking feature to block certain people from seeing posts, with this over-reliance stemming from their lack of knowledge of all available privacy settings. When asked if they knew of any other privacy settings, for example, P6 stated that blocking was the *'only thing she could think of'* to prevent others from seeing their content. For example, one participant explicitly stated that the reason he preferred WhatsApp to Facebook is because it is not possible to block people from seeing posts on Facebook, whereas he can on WhatsApp.

P18: That's because I can block my mom and aunts from seeing my WhatsApp status updates and I cannot block them from seeing my posts on Facebook.

Our participants also did not fully grasp the granular nature of privacy settings on Facebook and therefore, they acted in an absolute manner of blocking people from everything.

4.2.3 Users Often Manage Privacy And Phone Sharing

The majority of the participants reported that their access to social media was restricted by the *'WiFi limit'* or their data limit on their mobile devices, which others noted affects Internet usage [40, 53]. Most of the participants interviewed in the townships only used their mobile phones for social media access or used free Internet at a library, some visited Internet cafes, or went online by borrowing a friend or family member's phone or in a few cases, a laptop at work. Thus, phone sharing, a common practice amongst individuals from lower income backgrounds [48] was mentioned frequently. Participants in our study, similar to those in a study conducted in Bangladesh [4], commonly shared their phones with others. Often, sharing occurred between parents and children or significant others. Participants also talked about borrowing a friend's phone or lending their phone to others whose data had run out. Therefore, our participants expressed concerns about privacy issues stemming from physical access of the phone, such as people they know accessing their private social media account information on their own or shared devices.

In our study, participants mentioned managing privacy by deleting messages immediately after texting with someone, or putting passwords on apps so that their children had to ask for the password to access specific apps. This self curating behavior was also noted in South Asia by women who felt they had few other ways to manage privacy, especially on shared devices, and was also reflected in Indian privacy attitudes [36, 57]. Regarding social media privacy and phone sharing specifically, for many users, there was a concern about saved/auto-login features, features that save passwords on applications, that assume that only a single user accesses the system. One participant, when asked if she experienced a privacy breach, explained how auto-login could be an issue:

P26: There was a time that I didn't have a phone and I used to login on other people's phones. So people [logged in as me and] started posting nasty stuff and upset other people on my behalf.

At least 5 participants reported that they logged out of social media when accessing it on other people's devices because they were afraid of other people going through their personal profiles and messages. Even if the participant remembered to logout from the application, access to the phone could still be enough to "prove" that the person who is on the device trying to log in is the same as the social media account holder.

P3: There was a time when, my girlfriend at the time, she went onto my Facebook. I was logged off. She clicked 'forgot password'. And when you click forgot password, it goes to your email which was on my phone. And then, she changed my password. I wasn't even there, but that happened. She changed the password, accessed my Facebook, and read my messages.

One or two of the individuals we interviewed tried to use a combination of settings and tools, such as password locks on the applications themselves through the use of a third-party app "App Locker" to prevent others from accessing their accounts. This echoes findings from South Asia where women would often use app locking applications to manage their privacy on devices that they share, often with a significant other with a power dynamic dictating they offer full access to their content [57]. However, those participants who knew of such settings or tools to enhance their privacy often decided not to use them, explaining that the privacy they gained was not worth the inconvenience of having to spend extra time logging in to each application.

4.3 Crime And Social Media Behaviors

Many of our participants shared that offline concerns heavily influenced their online privacy practices and feelings of security online and in person. That is, physical safety concerns led them to change both how they viewed and used social media and shaped their mental models of privacy on social media.

4.3.1 Physical Danger And Social Media Posts

A concerning trend mentioned by some participants was the tendency of criminals in their area to track people's whereabouts through social media activity. In particular, participants mentioned that via catfishing, the practice of creating a false identity online to deceive others, and other forms of social engineering, malicious actors were luring others to more private locations and then either raping or kidnapping them. In a typical quote about these scams online, participant P25 said:

P25: It's the scams that people do on Facebook; I've heard of people luring other people with fake job opportunities and kidnapping or raping them.

Others discussed encountering fake job vacancies posted to get people isolated where they could be robbed. Participants mentioned many other instances of crime. For instance, one participant in Khayalitsha told of how she had been robbed at least 4 times at gunpoint, with the assailants shooting at her and stealing her phone. Another participant talked about her son being stabbed; others talked about looking for news online about car hijackings in the area or using social media to contact a cousin whose house, a *'shipping container'*, had burned down. Another talked about leaving their phone at home to avoid getting mugged on their way to school.

Owing to crime being part of daily life, many participants gave examples of how it affected their social media behaviors. One participant mentioned that she delayed posting pictures

on social media until one or two days after they are taken to ensure nobody learns where she is in real-time. Another participant spoke about how some people take the precaution of not posting pictures of their children's school uniform, to try to hide where his children went to school from potential kidnappers. One of the other participants discussed ensuring his location was always turned off on social media so that robbers would not know when he was away from home. In a few cases, participants mentioned how they shared their passwords for their accounts with family members in case something happened to them. For instance, one participant told us how their father can access her Facebook account in case of 'kidnapping' so that they could be tracked down:

> P32: Even my email address my dad knows the password and when I used to a have a phone my dad used to log in on my WhatsApp. The reason is that if something happens to me like suicide or kidnapping, it will help with the investigation. As in, maybe this is what caused her to commit suicide. Maybe they will see if I was going to meet up with someone when I was kidnapped.

In another case, a mom talked about sharing her passwords with her children so they could still access the shared phone if *'something happens to me'*. Participants also spoke of how Facebook was useful in high-crime areas. For instance, for helping to track missing persons and advocating for a cause. One person used it to find a cousin that had gone missing.

> P15: For instance, at one time, my cousin just disappeared and no one knew where she was was but because I knew her surname, I searched for her on Facebook and we could locate her whereabouts. Also, when there's a missing person you can post their picture on Facebook and there are groups that help in situations like that.

Participants clearly did not always want real-time posting to avoid physical threats resulting from others seeing their live information. Crime also affected how users used social media and what compromises they made to allow others to find them in case something happened to them.

4.3.2 Frequent Account Hacking

At least 12 participants talked about their Facebook accounts being hacked at some point, requiring them to change their password. For example, two of the participants expressed concern that by gaining access to their passwords, bad actors would be able to take over their social media accounts and impersonate them. Participant accounts were hacked in numerous ways. In some cases, participants talked about forgetting to log out at Internet cafes and having their accounts hacked. In other cases, participants found out about the hacking by seeing activity on their accounts they did not engage in as P1 summarizes:

> P1: On Facebook there was this one time where my friend's profile, sent me a link to a video of myself. I opened the link, and then next thing I knew, my Facebook profile was commenting on people's photos. I have no clue how that happened, but then I changed my password and it was fine.

In other cases, participants were alerted to hacking by friends as in the case of P39:

> P39: My Facebook had this thing where I could not log in and I did not know why. Then I got complaints from my friends that someone is using my Facebook and I wondered: how do these people get onto other people's Facebook accounts? And these fake people are setting up in meetings asking my friends to meet up somewhere. The thing is that person [who was contacted] had called me because the person that was using my Facebook had mentioned a location that I've never been to, so that person was wondering what [was] going on.

In another case, a participant told us how someone had set up an account with her cousin's pictures and how she had to help her cousin report the fake account to Facebook, equating the outcome as Facebook being able to *'block the person'*. Sometimes even if participants tried to deal with the hacking, data issues prevented them from doing so as P39 told us that when he tried to report this incident to Facebook *'There was just a lot that I had to read there and my data was getting finished so I decided to just log out'*. They eventually gave up and started a new account instead. Overall, participants often had difficulties with rampant account hacking.

4.3.3 Frequent Encounters of Inappropriate Or Crime Related Content

Interestingly, participants not knowing a lot about privacy settings also were left exposed to inappropriate content more often than desired. Over a third of participants told us of frequently encountering inappropriate content on their social media accounts including nudity, pornography, and posts with physical violence. For instance, participants mentioned receiving pornographic messages and videos on WhatsApp groups or on WhatsApp as well as seeing pornographic content on Facebook. In one case, a participant joined a group 'Looking for love' only to find out that instead of being associated with the radio show they loved, sexual content was being shared so they had to leave 'immediately'.

> P50: People take advantage and post nonsense. They don't care what they post. Some of them even post inappropriate private stuff. Things we should not see about them.
> I: Have you ever come across a content that you did not want to seen on Facebook?
> P50: Yes, porn videos and people post whatever

they feel like posting. Some of the things they post are just not appropriate for one to see.

Often, participants did not know how to deal with these encounters or how to avoid this content. Sometimes these pictures were crime related, other times it was pictures of injuries or other disturbing images. For instance, P15 told us of seeing a picture of a woman who was brutally murdered by her husband and how it was *'seriously disturbing'* and P25 mentioned seeing posts of *'people cutting children's throats'*. In another example, P18 spoke of:

> P18: I have seen a picture of a little baby in a plastic bag before and a picture of a child who was burnt very badly. The caption on the picture of the burnt child was asking for donations and help, that post left me very disturbed. On those type of posts, it asks you if you want to see the post again and then I normally click the no option.

These posts often scared participants and made them feel bad after viewing the content. In some cases, they were false alarms such as people posting fake content about others passing away and it turning out to be 'all lies' which was harrowing for participants living in a high-crime setting. In other cases, participants talked about seeing nudity or being the victims of revenge postings with sexual content about them.

> P13: One time my friend called me and told me to go and search for a particular person and I did that and that person stays here in Langa and I saw pictures of them naked.
> I: what did you to stop that?
> P13: I stopped searching for that person.

In some cases, this inappropriate content appeared on Status messages which participants had no control over. For instance, in one case, a participant spoke of seeing that a contact had put a message on their Status about the father of their children beating them up. In most of these cases, participants spoke of just *'taking a break'* from the platform or waiting for the Status message to disappear after 24 hours since there was no other way to avoid this content. Some participants spoke of having to just *'scroll past and log out'* to avoid the content or logging off and taking a break to avoid seeing this content.

4.3.4 Social Media As Data Storage In Case Of Theft

A final theme that emerged from the interviews, particularly with the lower-income individuals, was the usage of social media platforms as a means of data storage to save information. Participant used social media in this way due to the rampant phone theft issues in South Africa, with more than 475,000 reported cell phone thefts this past year [27] and living in high-crime areas. These participants explained that they wanted to ensure that even if their devices were stolen, they would still have access to the precious memories stored in pictures. In a typical example, one participant, P45, shared the following reason about which pictures she posts on Instagram:

> P45: I only post the pictures that I like and think are nice. I also ensure that I post the pictures I would like to have even after my phone has gone missing.

Another reason participants uploaded their images to social media was owing to phone memory issues or in the event that a phone malfunction occurred. At least 7 lower-income participants reported that one of their primary uses for social media was to upload their pictures to either Facebook or Instagram for later retrieval. One participant, P49, explained her reasoning for this logic as an issue with how pictures were currently being stored on her device.

> I: Why do you post your pictures on Facebook?
> P49: I want to keep them.
> I: Oh so why do you keep them on Facebook? Why can't you keep them somewhere else?
> P49: Memory cards have issues sometimes they reformat themselves.
> I: And Facebook never reformats?
> P49: Never

That being said, those who employed this strategy admitted that there were negative repercussions of their uploading all of their photos to Facebook or Instagram, including not internalizing that what they post on Facebook is unlike a storage platform by its very nature. For example, in one interview, a participant mentioned her concern over the fact that anything she uploaded for "storage" on Facebook would be able to be seen by others, limiting her control over privacy.

> I: What would make you want to use Facebook again?
> P43: If there was a guarantee that my pics cannot be downloaded, then it would be fine.
> I: Why is protection of pictures so important to you?
> P43: For the sake of my privacy. So that nothing negative can be circulated about me.

Using social media as a means to preserve their data in the event of phone theft is one example of the intersection between physical and digital privacy for our participants.

5 Discussion

Our findings show that users were primarily concerned about other individuals seeing their posts, but did not know how to control information visibility on social media platforms. Moreover, our findings suggest that users struggled to manage their privacy, particularly in contexts of shared devices. Our findings also demonstrated that physical safety threats caused our participants to desire non-real time posting and use social media for data storage. Participants also experienced frequent account hacking and were often encountering crime-related

content on social media that was sometimes disturbing. Based on our findings, we make the following recommendations for future work.

5.1 Challenge "Always online" Assumptions

Our study suggests that we need to challenge assumptions about 'typical' users when designing privacy and security settings such as that users are always online or have reliable, frequent access to the Internet. These assumptions can disadvantage users in resource-constrained settings with high data costs. For example, recovering from an account hacking is difficult if it requires you to follow a lengthy process that requires constant connectivity. Additionally, the process of changing privacy settings can also be lengthy; on WhatsApp, which nearly all of the participants described as being better for privacy than Facebook, navigating to the privacy settings takes 2 clicks. On Facebook, the same process requires 3-4 clicks, depending on which route is taken. A suggestion would be to bring those settings forward on all social media sites, which could increase the knowledge and usage of the privacy settings. Resource-constrained users could also benefit from lightweight privacy on-boarding interfaces and privacy and security settings that can be configured offline. Designers could also help users glean privacy-management related information from their social contacts when users are online. Users could also be provided with familiar ways of finding out information. For instance, an informational 'WhatsApp' chat-bot contact that will reply to natural language questions with the desired information about privacy or security could work well in these settings. Finally, most of our participants rarely altered settings from their default states confirming other studies [24, 38]. Therefore, making posts more private by default might be more apt in helping less tech-savvy users maintain privacy.

5.2 Improve Data Compartmentalization On Devices

Our participants, like others in settings where device sharing is common, often encountered security and privacy issues owing to shared devices. The security community could aid with this issue by designing better ways to compartmentalize data storage and access on a phone that is easy for a user to understand, use, and manage. This underlying infrastructure should afford users the ability to easily grant access to parts of the device or data without causing social awkwardness or overtly challenging power dynamics that are hard to avoid. This requires technical innovation and further user studies.

5.3 Accommodate Use In High-Crime Areas

Finally, our participants were often concerned with their physical safety. Future work could examine if non-real time posting would alleviate some physical safety concerns by allowing users to schedule posts for later times. Systems to alert users if their posts contain personal information that could be misused or obfuscate certain information could also be beneficial in high-crime settings. Further work is also needed to understand how to improve content moderation mechanisms for high-crime areas where inappropriate content and misinformation spread unchecked on social media platforms. For instance, future work could examine how to help users, particularly on WhatsApp, better report and flag inappropriate content and overcome susceptibility to hacking from sharing phones.

6 Study Limitations

Our study had a sample size of 52 users only. Additionally, all of the participants, while living in different regions of the city, all lived in Cape Town, South Africa. Further, interviews were conducted in a semi-structured manner, meaning that just because participants may not have explicitly discussed something, that does not preclude them from having a viewpoint on that subject. Lastly, due to the number of interviews and the coding process used (3.4), it is possible that a participant mentioned something that was not picked up during our coding process. Our study can be extended to a wider demographic in other settings with low income individuals. Future work could investigate current privacy behaviors on other social media platforms in depth (e.g., examining the difference in preferences on WhatsApp versus Facebook) to see how privacy can be better attained through different types of settings and which settings are most appropriate for marginalized settings.

7 Conclusion

Our study demonstrated that South African mobile users primarily worry about who has access to their online data on social media. Our participants were generally unaware about granular privacy settings on social media platforms and had to manage posting personal information in a high-crime area that could mark them as a target. Our findings suggest the security community needs to better accommodate users in resource-constrained settings, improve data compartmentalization on devices, and design to help users in high-crime areas use social media safely. Future work could implement the suggested design recommendations and evaluate their effectiveness at improving privacy and security management for users in resource-constrained settings.Future studies could investigate people's knowledge of privacy breaches and online tracking in resource-constrained settings.

8 Acknowledgements

This work was supported by a Facebook Securing the Internet grant. We thank Minah Radebe for research assistance, our participants, and reviewers.

References

[1] Top Sites in South Africa. *Alexa*, 2019.

[2] Standing A. The social contradictions of organised crime on the cape flats. *Institute for Security Studies Papers*, 74(1):16–16, 2003.

[3] Norah Abokhodair and Sarah Vieweg. Privacy & social media in the context of the arab gulf. *DIS '16*, pages 672–683, 2016.

[4] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. Digital privacy challenges with shared mobile phone use in bangladesh. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW):17:1–17:20, December 2017.

[5] Tawfiq Alashoor, Arun Aryal, and Grace Fox. Understanding the privacy issue in the digital age: An expert perspective. *AMCIS*, 08 2016.

[6] Athanasios Andreou, Giridhari Venkatadri, Oana Goga, Krishna P Gummadi, Patrick Loiseau, and Alan Mislove. Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations. *NDSS 2018*, pages 1–15, February 2018.

[7] David Armstrong, Ann Gosling, John Weinman, and Theresa Marteau. The place of inter-rater reliability in qualitative research: an empirical study. *Sociology*, 31(3):597–606, 1997.

[8] Susanne Barth and Menno D.T. de Jong. The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. *Telematics and Informatics*, 34(7):1038 – 1058, 2017.

[9] Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle L. Mazurek, Michael K. Reiter, Manya Sleeper, and Blase Ur. The post anachronism: The temporal dimension of facebook privacy. *WPES '13*, pages 1–12, 2013.

[10] France Bélanger and Robert E. Crossler. Privacy in the digital age: A review of information privacy research in information systems. *MIS Q.*, 35(4):1017–1042, December 2011.

[11] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the internet goes down in bangladesh. *CSCW '17*, pages 1591–1604, 2017.

[12] Hsuan-Ting Chen. Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, 62(10):1392–1412, 2018.

[13] Jay Chen, Michael Paik, and Kelly McCabe. Exploring internet security perceptions and practices in urban ghana. *SOUPS 2014*, pages 129–142, 2014.

[14] Hichang Cho and Anna Filippova. Networked privacy management in facebook: A mixed-methods and multinational study. *CSCW*, pages 503–514, 2016.

[15] Hichang Cho, Bart Knijnenburg, Alfred Kobsa, and Yao Li. Collective privacy management in social media: A cross-cultural validation. *ACM Trans. Comput.-Hum. Interact.*, 25(3):17:1–17:33, June 2018.

[16] J. Clement. South africa facebook messenger users by age 2019. *Statista*, Jan 2020.

[17] Gabriel J.X. Dance, Michael LaForgia, and Nicholas Confessore. As facebook raised a privacy wall, it carved an opening for tech giants. *The New York Times*, Dec 2018.

[18] Cobus de Swardt, Thandi Puoane, Mickey Chopra, and Andries du Toit. Urban poverty in cape town. *Environment and Urbanization*, 17(2):101–111, 2005.

[19] Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1):83–108, 2009.

[20] C. Dwyer. Privacy in the age of google and facebook. *IEEE Technology and Society Magazine*, 30(3):58–63, Sep 2011.

[21] Michaelanne Dye, David Nemer, Laura R. Pina, Nithya Sambasivan, Amy S. Bruckman, and Neha Kumar. Locating the internet in the parks of havana. *CHI '17*, pages 3867–3878, 2017.

[22] Sebastiana Etzo and Guy Collender. The mobile phone 'revolution' in Africa: Rhetoric or reality? *African Affairs*, 109(437):659–668, 08 2010.

[23] Erving Goffman. *The presentation of self in everyday life*. N.Y.:Doubleday, 1959.

[24] Daniel G. Goldstein, Eric J. Johnson, Andreas Herrmann, and Mark Heitmann. Nudge your customers toward better choices. *Harvard Business Review*, 86(12):99–105, December 2008.

[25] Rebecca Greenfield. 2012: The year facebook finally tried to make some money. *The Atlantic*, Dec 2012.

[26] Graham Greenleaf. Global data privacy laws 2017: 120 national data privacy laws, including indonesia and turkey. *145 Privacy Laws & Business International Report*, Jun 2017.

[27] Riaan Grobler. Crime by numbers - everything you need to know about the latest stats.

https://www.news24.com/SouthAfrica/News/crime-by-numbers-everything-you-need-to-know-about-the-latest-stats-20181011, Oct 2018.

[28] Todd Haselton. How to delete messages you regret sending on facebook messenger, just like mark zuckerberg. https://www.cnbc.com/2019/02/05/how-to-delete-messages-on-facebook-messenger.html, Feb 2019.

[29] Paul Hitlin and Lee Rainie. Facebook algorithms and personal data. *Pew Research Center*, Jan 2019.

[30] Gordon Hull, Heather Richter Lipford, and Celine Latulipe. Contextual gaps: privacy issues on facebook. *Ethics and Information Technology*, 13(4):289–302, Dec 2011.

[31] Maritza Johnson, Serge Egelman, and Steven M Bellovin. Facebook and privacy: it's complicated. *SOUPS*, page 9, 2012.

[32] Evangelos Karapanos, Pedro Teixeira, and Ruben Gouveia. Need fulfillment and experiences on social media. *Comput. Hum. Behav.*, 55(PB):888–897, February 2016.

[33] Jason Kaufman, Kevin Lewis, and Nicholas Christakis. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, 14(1):79–100, 10 2008.

[34] Simon Kemp. Global digital report 2019. *We Are Social*.

[35] Jennifer King, Airi Lampinen, and Alex Smolen. Privacy: Is there an app for that? *SOUPS*, page 12, 2011.

[36] Ponnurangam Kumaraguru and Niharika Sachdeva. Privacy in india: Attitudes and awareness v 2.0. 2012.

[37] Sebastian Labitzke, Florian Werling, Jens Mittag, and Hannes Hartenstein. Do online social network friends still threaten my privacy? *CODASPY '13*, pages 13–24, 2013.

[38] Wendy E. Mackay. Triggers and barriers to customizing software. *CHI '91*, pages 153–160, 1991.

[39] Douglas MacMillan and Robert McMillan. Google exposed user data, feared repercussions of disclosing to public. https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194, Oct 2018.

[40] Arunesh Mathur, Brent Schlotfeldt, and Marshini Chetty. A mixed-methods study of mobile users' data usage practices in south africa. *UbiComp '15*, pages 1209–1220, 2015.

[41] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[42] Gugulethu Mhlungu. All you need to know about stokvel. *News24*, Dec 2017.

[43] D. Miller. *Tales from Facebook*. Wiley, 2011.

[44] Moses Namara, Daricia Wilkinson, Byron M Lowens, Bart P Knijnenburg, Rita Orji, and Remy L Sekou. Cross-cultural perspectives on ehealth privacy in africa. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, page 7. ACM, 2018.

[45] Lily Hay Newman. A new google blunder exposed data from 52.5 million users. https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/, Dec 2018.

[46] Phillip Nyoni and Mthulisi Velempini. Data protection laws and privacy on facebook. *SA Journal of Information Management*, 17(1):10, 2015.

[47] Phillip Nyoni and Mthulisi Velempini. Privacy and user awareness on facebook. *South African Journal of Science*, 114(5/6), 2018.

[48] Erick Oduor, Carman Neustaedter, Tejinder K. Judge, Kate Hennessy, Carolyn Pang, and Serena Hillman. How technology supports family communication in rural, suburban, and urban kenya. *CHI '14*, pages 2705–2714, 2014.

[49] Sarah Perez. Messenger lite launches on ios, but only in turkey. https://techcrunch.com/2018/10/09/messenger-lite-launches-on-ios-but-only-in-turkey/, Oct 2018.

[50] Jacob Poushter, Caldwell Bishop, and Hanyu Chwe. Social media use continues to rise in developing countries, but plateaus across developed ones. *Washington: Pew Internet and American Life Project*, 6 2018.

[51] Yasmeen Rashidi, Kami Vaniea, and L. Jean Camp. Understanding saudis privacy concerns when using whatsapp. *Proceedings 2016 Workshop on Usable Security*, Feb 2016.

[52] Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos. Sharing ephemeral information in online social networks: Privacy perceptions and behaviours. In *INTERACT 2011*, pages 204–215. Springer Berlin Heidelberg, 2011.

[53] Julianne Romanosky and Marshini Chetty. Understanding the use and impact of the zero-rated free basics platform in south africa. *CHI '18*, pages 192:1–192:13, 2018.

[54] Johnny Saldañna. *The Coding Manual for Qualitative Researchers*. SAGE, Los Angeles, 2nd ed edition, 2013.

[55] Saima Salim. "how much time do you spend on social media? research says 142 minutes a day". *Digital Information World*, January 2019.

[56] Nithya Sambasivan, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. 'they don't leave us alone anywhere we go': Gender and digital abuse in south asia. *CHI '19*, pages 2:1–2:14, 2019.

[57] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. *SOUPS 2018)*, pages 127–142, 2018.

[58] Toby Shapshak. Almost all of facebooks 139 million users in africa are on mobile. *Forbes*, Dec 2018.

[59] We Are Social. Digital in 2018 in southern africa, slide 85, Jan 2018.

[60] We Are Social. Most popular social networks worldwide as of january 2019, ranked by number of active users (in millions). *Statista - The Statistics Portal*, Jan 2019.

[61] Jennifer Jiyoung Suh, Miriam J. Metzger, Scott A. Reid, and Amr El Abbadi. Distinguishing group privacy from personal privacy: The effect of group inference technologies on privacy perceptions and behaviors. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW):168:1–168:22, November 2018.

[62] The New York Times. Mark zuckerberg testimony: Senators question facebook's commitment to privacy. https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html, Apr 2018.

[63] David Muli Tovi and Mutua Nicholas Muthama. Addressing the challenges of data protection in developing countries. *European Journal of Computer Science and Information Technology*, 1:1–9, 09 2013.

[64] Sabine Trepte, Doris Teutsch, Philipp K. Masur, C Eichler, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)*, pages 333–365. 01 2015.

[65] Zeynep Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008.

[66] Momentum Unisa. 2017 financial wellness index summary, 2017.

[67] Blase Ur, Manya Sleeper, and Lorrie Faith Cranor. {Privacy, Privacidad,...} policies in social media: Providing translated privacy notice. In *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, page 6. ACM, 2012.

[68] Blase Ur and Yang Wang. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22Nd International Conference on World Wide Web*, WWW '13 Companion, pages 755–762, New York, NY, USA, 2013. ACM.

[69] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining security and privacy research in developing regions. *COMPASS '18*, pages 25:1–25:14, 2018.

[70] Aditya Vashistha, Abhinav Garg, Richard Anderson, and Agha Ali Raza. Threats, abuses, flirting, and blackmail: Gender inequity in social media voice forums. *CHI '19*, pages 72:1–72:13, 2019.

[71] Na Wang, Heng Xu, and Jens Grossklags. Third-party apps on facebook: Privacy and the illusion of control. *CHIMIT '11*, pages 4:1–4:10, 2011.

[72] Na Wang, Heng Xu, and Jens Grossklags. Third-party apps on facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM symposium on computer human interaction for management of information technology*, page 4. ACM, 2011.

[73] Jason Watson, Heather Richter Lipford, and Andrew Besmer. Mapping user preference to privacy default settings. *ACM Trans. Comput.-Hum. Interact.*, 22(6):32:1–32:20, November 2015.

[74] Zack Whittaker. Facebook admits it stored 'hundreds of millions' of account passwords in plaintext. *TechCrunch*, Mar 2019.

[75] Susan Wyche. Exploring mobile phone and social media use in a nairobi slum: A case for alternative approaches to design in ictd. *ICTD '15*, pages 12:1–12:8, 2015.

[76] Susan Wyche and Eric PS Baumer. Imagined facebook: An exploratory study of non-users' perceptions of social media in rural zambia. *New Media & Society*, 19(7):1092–1108, 2017.

[77] Susan P. Wyche, Andrea Forte, and Sarita Yardi Schoenebeck. Hustling online: Understanding consolidated facebook use in an informal settlement in nairobi. *CHI '13*, pages 2823–2832, 2013.

[78] Susan P. Wyche, Sarita Yardi Schoenebeck, and Andrea Forte. "facebook is a luxury": An exploratory study of social media use in rural kenya. *CSCW '13*, pages 33–44, 2013.

[79] Alyson L. Young and Anabel Quan-Haase. Information revelation and internet privacy concerns on social network sites: A case study of facebook. *C&T '09*, pages 265–274, 2009.

A Interview Guide and Codebook

Mobile Data And Phone Details

Q1: What type of phone do you own and use? How long have you had this device?
Q2: What mobile data plan do you have? Why? How long have you been on this plan?
Q3: Which activities do you most commonly use your phone for? Why? When? How often?
Q4: Which social media sites do you most often visit online? Why? When? How often?

Social Media General Usage Patterns

Q5: When did you start using <social media app(s)>? Why? What do you like about it/them? What do you dislike about it?
Q6: How are your contacts on the app? How many do you think you have? Are there any contacts you did not want to add? Why?
Q7: Do you use <social media app(s)> on your mobile phone only? Where else do you use it? Why?
Q8: Is there anything you avoid doing on social media? What? Why?
Q9: Is there anything you do on social media that you do not do on other apps? What?
Q10: Have you ever considered not using your <social media app(s)> anymore? Why/why not?
Q11: Have you ever heard criticisms of your social media app, or other social media apps? What were they? Have they affected you? Have these affected your usage in any way?
Q12: Which of the social media apps you use do you believe is most compatible with your views on privacy?

Privacy on Social Media

Q13: How much do you trust the company that made <social media app>? Why/why not?
Q14: Who do you think can see your profile on <app>?
Q15: Have you thought about who can see what you're sharing/posting on <app>?
Q15.1: Who do you think can see the content you share?
Q15.2: Who do you share with most/least often? Why?
Q15.3: Do you share more or less on some apps? Why?
Q15.4: Have you ever changed what you post to maintain your privacy? What did you do? Why?
Q15.5: Have changed who can see what you post to maintain your privacy? What did you do? Why?
Q16: Have you thought about who can see what posts/content/videos you are seeing on a social media platform?
Q16.1: Who else do you think can see what you see on your apps <ask about each app>?
Q16.2: Tell me if anyone has ever blocked you from seeing content? Why?
Q16.3: Have you ever seen content you did not want to see? What did you do to stop it?
Q17: Have you ever shared your password for <app>? Why/why not?
Q18: Have you ever shared your phone with someone else?
Q18.1: Do you think that the person who used/uses your phone can see what you do on <app>? How does that make you feel?
Q18.2: Do you change what you do on the <app> because you share your phone?
Q19: Tell me about whether you think <app name> collects any information about you?
Q19.1: What information do you think they collect?
Q19.2: Why do you think they collect this information?
Q20: Are you aware of any settings on any of the social media platforms <say the names> that you use that can change who can see what you post?
Q20.1: For each app, have you ever used these settings?
Q20.2: How/When/Why did you use them?

Privacy in General

Q21: What does privacy on the Internet mean to you?
Q22: How do you maintain your privacy when you go on the Internet? Does it differ based on device?
Q23: Are there any tools you use to help you keep private on the Internet? What? When/why do you use them? Which devices do you use these tools on?
Q24: Tell me about some instances in which you felt your privacy was breached on one of your social media apps <use actual names>?
Q24.1: Which app? What happened? Why do you think it happened? Did you take any measures to prevent this from happening again?
Q25: Tell me about how your privacy practices differ depending on which application you are using?
Q26: Are you aware of privacy settings in any of the social media apps you use? Can you tell me more about how you use them on each app? Can you show me these settings?

Topic/Code	**Sub-topic/Child Code**
GENERAL	
Activities On Phone	
Definition Of Privacy	
Lack Of Data	
GENERAL SOCIAL MEDIA USAGE	
Contacts On Social Media	
Method Of Access	
Platform/Company-specific Thoughts/Behavior	*(Explicit) intimacy of WhatsApp*
	Sharing on some platforms, not others
	Trust of company affects behavior
Reason For Dislike Of Social Media	
Reason For Liking/Using Social Media	
PRIVACY, SECURITY, AND USAGE	
Concern About People Seeing/Inferring Things (Or Too Much)	*Intimate personal info (family, medical, etc.)*
	Family
	Work/Professional Contacts
Crime	*See crime related news*
Inappropriate Content	
Phone Sharing	*Concern about privacy infringement*
	Shares login information/account
Privacy Related Behavior	*Avoid certain behaviors*
Thoughts/Actions Regarding Who Can See Posts	*Skepticism about how private it is*
	Usage of private setting
	Usage of blocking feature
Thoughts About Advertisements/Tracking	*Expressed concern over advertisements*
	Knowledge (or lack thereof) of ad-tracking
Unwanted Contact	
Use Of Tools/Settings To Maintain Privacy	*Software solution*
	Usage of privacy settings

Table 3: Code Book With Main 17 Parent and 17 Child Codes (Note, we do not show sub-codes of child codes since these were not used in the main analysis.)