Security and Privacy Beyond Western Peripheries:
Practices, Challenges, and Opportunities in the Majority World

by Collins W. Munyendo

B.S. in Business Information Technology, May 2016, Strathmore University
M.S. in Information Technology, December 2018, Carnegie Mellon University

A Dissertation submitted to

The Faculty of
The School of Engineering and Applied Science
of the George Washington University
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

January 9, 2026

Dissertation directed by

Adam J. Aviv
Associate Professor of Computer Science

The School of Engineering and Applied Science of The George Washington University certifies that Collins W. Munyendo has passed the Final Examination for the degree of Doctor of Philosophy as of March 19, 2025. This is the approved form of the dissertation.

Security and Privacy Beyond Western Peripheries:
Practices, Challenges, and Opportunities in the Majority World

Collins W. Munyendo

Dissertation Research Committee:

Adam J. Aviv, Associate Professor of Computer Science,
Dissertation Director

Sibin Mohan, Associate Professor of Computer Science,
Committee Member

Gabriel Parmer, Professor of Computer Science,
Committee Member

Elissa M. Redmiles, Assistant Professor of Computer Science,
Committee Member

Yixin Zou, Tenure-Track Faculty,
Committee Member

© Copyright 2026 by Collins W. Munyendo
All rights reserved

Dedication

To my dad, Bruno Munyendo, for your endless support and encouragement. I miss you.

Acknowledgments

This dissertation would never have been possible without the mentorship and patience of my advisor, Adam Aviv. I will always be indebted to Adam for taking a chance on me and showing me how to conduct great research. Through Adam's guidance, I have grown both as a researcher and as a person. I also extend my gratitude to my committee members, Elissa Redmiles, Yixin Zou, Gabriel Parmer, and Sibin Mohan. When I was naively contemplating pursuing a PhD, Elissa was very kind and not only responded to my cold email, but also pointed me toward other professors. I am fortunate to have been mentored by her in the later stages of my PhD. I am equally grateful to Yixin for her mentorship and for the opportunity to spend some of my best summers in Germany working closely with her and her group.

I am very grateful to Michelle Mazurek who has always been there to offer me advice and guidance throughout my PhD. Thank you for your willingness to write me recommendation letters, even on very short notice. I also thank Yasemin Acar and Noel Warford for mentoring me early on in my PhD. The bouldering sessions and hikes with Yasemin were very important in keeping me sane. I am also grateful to Blase Ur who has especially been helpful in helping me overcome my impostor syndrome. I thank Aggrey Muhebwa for not just encouraging me to apply to PhD programs, but guiding me in the application process and the PhD journey as well. I could honestly dedicate a whole chapter in this dissertation to Aggrey.

I would also like to thank all my GWUSEC labmates and friends, including David Balash, Lucy Simko, Monica Kodwani, Adryana Hutchinson, Elena Korkes, Miles Grant, Xiaoyuan Wu, Jan Tolsdorf, Junho Eum, Wellington Barbosa, Arwa Alsahdi, Smirity Kaushik, Shiza Ali, Matthias Fassl, Jialiang Yan, Rafael Martinez, Joe Staller, Neal Keating, Mindy Tran, Harshini Sri Ramulu, Irwin Reyes, Hunter Dyer, Eddie Cosic, Rachel Rodriguez, Alvin Isaac, Darika Shaibekova, and Victoria Hennemann. I spent a significant part of my PhD closely working with Miles and Elena, and you were both a delight to work with. A big shout out to Lucy whose work on refugees was a big inspiration for me to pursue my PhD. I am going to really miss sitting next to Monica (my academic gossip partner) in the lab.

Throughout my PhD, I have been fortunate to collaborate with a lot of really amazing people, including Alexandra Nisenoff, Philipp Markert, Jaron Mink, Kentrell Owens, Kavous Salehzadeh Niksirat, Miranda Wei, Timothy Forman, Peter Mayer, Karen Sowon, Jackie Hu, Veronica Rivera, Amna Shahnawaz, Emmanuel Tweneboah, Marcos Silva, Yue Deng, Mercy Omeiza, Gayatri Priyadarsini, Dilara Keküllüoğlu, Daniel Bailey, Lily Klucinec, Luisa Ball Schnell, Cora Sula, Onicio Batista Leal Neto, Faith Strong, Shaoqi Wang, Franziska Herbert, Jonas Hielscher, Steffen Becker, Eunice Maingi, Gerald Suleh, Francisco Marmolejo-Cossio, Abhishek Bichhawat, Lorrie Cranor, Giulia Fanti, Conrad Tucker, Assane Gueye, Kurt Hugenberg, Tadayoshi Kohno, Gang Wang, Franziska Roesner, and Carmela Troncoso. I have learned a lot from all of you, and I look forward to working together more in future.

I am very grateful to everyone at the Max Planck Institute for Security and Privacy in Germany, especially members of the Human-Centered Security and Privacy Group including Johanna Gunawan, Gabriel Lima, Xinru Tang, Princessa Cintaqia, Kyle Beadle, and Priyasha Chatterjee as well as Maximilian Golla and Abraham Mhaidli. I always enjoyed our lunch time conversations (obviously about traveling in Europe) and are grateful that I remain in touch with most of you. I am also thankful to my friends at the SP2 Lab at UMD, including Wentao Guo, Julio Poveda, Phoebe Moh, Omer Akgul, Kelsey Fulton, Nathan Malkin, and Daniel Votipka. It was always easier to navigate conferences with some familiar faces.

Getting through a PhD has not been a walk in the park, and I am thankful for my PhD friends who have provided community, including Doreen Joseph, Joreen Arigye, Mir Masood Ali, Sarah Radway, Moses Namara, Kennedy Echesa, Daniel Nkemelu, Daniel Omeiza, Daniel Kemboi, Lin Kyi, Jenny Tang, Elijah Bouma-Sims, Hao-Ping Lee, Yaman Yu, Liz Ankrah, Joel Mugyenyi, Charity Delmus Alupo, Japheth Wambani, Lefu Maqelopo, and Nebiyou Yismaw. I would also like to thank all my friends at Nipe Sauti Africa and DC Bridges International for providing me a lot of encouragement. I am very grateful to Anne Namuli for always checking in on me, even when I was sometimes unresponsive. I will try to reach out more now that I am (hopefully) no longer constantly chasing deadlines.

I am deeply grateful to my family for their love and support throughout this journey. I am especially thankful to my dad, Bruno, for sacrificing everything for my education. You may no longer be here but I hope this dissertation will make you proud. I am also really grateful to my mum, Acquinata. Thank you for always checking in to make sure I survived winter. Some of my research, including the work on cybercafes, was directly inspired by you. I also thank my wonderful siblings, Pamela, Kevin, Linda, Maureen, and Maryline and my cousins, particularly Michelle, for cheering me through both the good and bad times.

Finally, I would like to thank all the agencies that funded this research, including the US National Science Foundation, Google through a Google PhD Fellowship, and the Stanford Internet Observatory, as well as all participants who generously took part in the studies that comprise this dissertation; this work would never have been possible without you!

Previous Papers

This dissertation is based on three previously published articles listed below. I have permission from my co-authors and publishers to use the works listed below in this dissertation. Copies of all copyright permissions are available in Appendix D.

- Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In Proceedings of the 43rd IEEE Symposium on Security and Privacy, Pages 2304-2319, San Francisco, CA, USA. May 2022 [102].

- Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In Proceedings of the 44th IEEE Symposium on Security and Privacy, Pages 570-587, San Francisco, CA, USA. May 2023 [103]. **Distinguished Paper Award.**

- Collins W. Munyendo, Veronica A. Rivera, Jackie Hu, Emmanuel Tweneboah, Amna Shahnawaz, Karen Sowon, Dilara Keküllüoğlu, Marcos Silva, Yue Deng, Mercy Omeiza, Gayatri Priyadarsini Kancherla, Maria Rosario Niniz Silva, Maryam Mustafa, Abhishek Bichhawat, Francisco Marmolejo-Cossio, Elissa M. Redmiles, and Yixin Zou. "I Wonder if These Warnings Are Accurate": Security and Privacy Advice in Nine Majority World Countries. To Appear in Proceedings of the 47th IEEE Symposium on Security and Privacy, San Francisco, CA, USA. May 2026 [106].

Abstract

Security and Privacy Beyond Western Peripheries: Practices, Challenges, and Opportunities in the Majority World

Human factors play a crucial role in the security and privacy ecosystem. However, most human-centered security and privacy research has focused on Western populations, despite evidence suggesting that security and privacy practices and needs differ across countries and cultures. As a result, security and privacy solutions designed for Western populations can fail when applied to other regions, leaving users at risk. In this dissertation, I explore the security and privacy challenges, practices, and needs of various majority world populations. I begin by examining concerns with mobile loan apps in Kenya, where their widespread use is driven by low socioeconomic status and a lack of formal credit history, making them a vital source of credit. Next, I broaden my scope to cybercafes, highlighting their role in digital access in Kenya and the privacy challenges that arise from sharing computing facilities. Finally, I extend my scope to multiple majority world countries, interviewing "local experts" across nine countries to understand security and privacy practices globally. Specifically, this dissertation investigates (i) privacy concerns and tradeoffs with mobile loan apps in Kenya, (ii) security and privacy challenges and practices at cybercafes in Kenya, and (iii) security and privacy concerns and advice in nine majority world countries.

To address these questions, I conducted three qualitative studies. First, I interviewed 20 users of mobile loan apps in Kenya to investigate why they use these apps, any privacy concerns they have with these apps, and how they navigate these concerns. To contextualize participants' sentiments, I additionally reviewed the data collection practices of common mobile loan apps, checking the permissions they request as well as how they indicate using users' data through their privacy policies. Afterward, I interviewed 14 managers and 22 customers of cybercafes in Nairobi, Kenya, inquiring about common security and privacy concerns and challenges customers face at those facilities, as well as the advice and support that is provided to them. To understand security and privacy concerns and advice

more globally, I finally interviewed 70 "local experts" across nine majority world countries spanning four continents, i.e., Africa (Kenya, Nigeria, and Ghana), Latin America (Mexico and Brazil), Asia (China, India, and Pakistan), and the Middle East (Türkiye).

My work shows that financial adversity in the majority world often makes users de-prioritize their privacy concerns, with many users of loan apps overlooking their privacy concerns to secure loans. My research further highlights how the reliance on "local experts" such as cybercafe managers for advice can expose users to security and privacy risks. For instance, some cybercafe managers encourage users to use simple passwords such as their names or ID numbers to avoid forgetting them, putting their security at risk. Additionally, I show how various factors in the majority world influence both the security and privacy concerns people have and their ability (or inability) to implement recommended advice. For example, cultural and religious norms often compel individuals to share their devices, undermining security and privacy measures designed in the West where device sharing is less common. Financial constraints also make it challenging for people to follow advice such as regularly updating their devices as these updates often require purchasing internet.

From these findings, I distill several recommendations. For apps like loan apps, I argue that stricter regulation by lawmakers and app markets is necessary to protect users' privacy as many users are willing to overlook their privacy concerns for loans. I also emphasize the need for more education and security awareness while challenging the efficacy and applicability of Western-designed solutions in the majority world. Ultimately, my work shows the need for continued research to better understand diverse user groups in the majority world in order to design security and privacy solutions that protect users globally.

Table of Contents

Dedication . . . . . **iv**

Acknowledgments . . . . . **v**

Previous Papers . . . . . **viii**

Abstract . . . . . **ix**

List of Figures . . . . . **xv**

List of Tables . . . . . **xvii**

1 Introduction **1**

1.1 Research Questions 2
1.2 Overview of Key Results and Takeaways 3
1.3 User Concerns with Mobile Loan Apps in Kenya 4
1.4 Security and Privacy Challenges and Practices at Cybercafes in Kenya 6
1.5 Security and Privacy Advice in the Majority World 7
1.6 Organization 9

2 Related Work **10**

2.1 Android Phone Permissions 10
2.2 Mobile Loan Apps and Other Digital Lenders 12
2.3 Cybercafes and Public Libraries 13
2.4 Security and Privacy Advice 14
2.5 Cross-National Security and Privacy Studies 16
2.6 Security and Privacy in the Majority World 17

3 Security and Privacy Concerns with Mobile Loan Apps in Kenya **19**

3.1 Introduction 20
3.2 Background on Mobile Loan Apps 23
3.2.1 About Mobile Loan Apps 23
3.2.2 How Mobile Loan Apps Work 24
3.2.3 Common Mobile Loan Apps in Kenya 25
3.2.4 Permissions Required by Mobile Loan Apps 26
3.2.5 Privacy Policies of Mobile Loan Apps 27
3.3 Methodology 28
3.3.1 Recruitment and Demographics 28
3.3.2 Interview Procedure 30
3.3.3 Data Collection 31
3.3.4 Data Analysis 31
3.3.5 Limitations 31
3.3.6 Ethical Considerations 32

3.4 Results . . . 33
3.4.1 Reasons for Use of Mobile Loan Apps . . . 33
3.4.2 User Perception of their Credit Score Calculation . . . 34
3.4.3 User Understanding of Permissions . . . 35
3.4.4 User Concerns with Mobile Loan Apps . . . 39
3.4.5 Privacy vs Loan Tradeoffs . . . 44
3.4.6 User Behaviour and Suggestions . . . 45
3.5 Discussion and Conclusion . . . 46
3.5.1 Importance of Loan Apps in the Majority World . . . 46
3.5.2 Concerns with Mobile Loan Apps . . . 47
3.5.3 Privacy versus Loan Tradeoffs . . . 47
3.5.4 (Mis)understanding of Permission Use . . . 48
3.5.5 User Education . . . 48
3.5.6 Over-privilege of Mobile Loan Apps . . . 48
3.5.7 Recommendations . . . 49

4 Security and Privacy Challenges and Advice at Cybercafes in Kenya . . . 50

4.1 Introduction . . . 51
4.2 Background on Cybercafes in Kenya . . . 54
4.3 Methodology . . . 55
4.3.1 Recruitment and Demographics . . . 56
4.3.2 Interview Procedure . . . 56
4.3.3 Data Collection . . . 58
4.3.4 Data Analysis . . . 59
4.3.5 Limitations . . . 60
4.3.6 Ethical Considerations . . . 60
4.4 Results . . . 61
4.4.1 Role of Cybercafes in Kenya . . . 61
4.4.2 Challenges at Cybercafes . . . 64
4.4.3 Advice and Support at Cybercafes . . . 67
4.4.4 Top Three Security and Privacy Advice . . . 72
4.4.5 Concerns, Practices, and Behaviors . . . 74
4.5 Discussion and Conclusion . . . 77
4.5.1 Role of Cybercafes in Kenya . . . 77
4.5.2 Reliance on Cybercafe Managers . . . 78
4.5.3 Security-Usability Tradeoff . . . 78
4.5.4 Security and Privacy Advice in Non-Western Contexts . . . 79
4.5.5 Cybercafe Risks and Concerns . . . 80

5 Security and Privacy Advice in Nine Majority World Countries . . . 82

5.1 Introduction . . . 83
5.2 Methodology . . . 86
5.2.1 Country Selection . . . 86
5.2.2 Research Personnel . . . 87
5.2.3 Recruitment and Demographics . . . 88

5.2.4 Interview Procedure . . . 88
5.2.5 Data Collection . . . 91
5.2.6 Data Analysis . . . 91
5.2.7 Limitations . . . 92
5.2.8 Ethical Considerations . . . 92
5.3 Results . . . 93
5.3.1 Top Three Security and Privacy Advice . . . 93
5.3.2 Sources of Advice . . . 96
5.3.3 Concerns Addressed by Advice . . . 98
5.3.4 Reasons for Following Advice . . . 103
5.3.5 Challenges and Contextual Factors . . . 104
5.4 Discussion and Conclusion . . . 112
5.4.1 Main Takeaways . . . 113
5.4.2 Next Steps . . . 115
5.4.3 Final Thoughts and Future Work . . . 117

6 Conclusion and Future Work . . . 119

6.1 Summary of Key Findings . . . 119
6.1.1 Impact of Economic Factors on Security and Privacy . . . 119
6.1.2 Mismatch of Advice Between Western Experts and Local Experts . . . 120
6.1.3 Device-Sharing Practices versus Security and Privacy . . . 120
6.1.4 Impact of Socio-Demographic Factors on Security and Privacy . . . 121
6.1.5 Comparison of Findings in the Majority World to Western Contexts . . . 122
6.1.6 Lessons from Conducting Cross-National Research . . . 122
6.2 Future Directions . . . 123
6.2.1 Exploring Concerns and Advice From the Users' Perspectives . . . 123
6.2.2 Validating Qualitative Findings Through Large-Scale Studies . . . 124
6.2.3 Rethinking Authentication and Password Management . . . 125
6.2.4 Designing Security and Privacy for Shared Contexts . . . 125

Bibliography . . . 126

A Mobile Loan Apps . . . 141

A.1 Interview Script . . . 141
A.2 Codebook . . . 142

B Cybercafes . . . 144

B.1 Interview Script . . . 144
B.1.1 Interview Script - Cybercafe Managers . . . 144
B.1.2 Interview Script - Cybercafe Customers . . . 146
B.2 Codebook . . . 148

C Security and Privacy Advice in the Majority World . . . 152

C.1 Interview Script . . . 152

D Copyright Permissions . . . 155

D.1 Mobile Loan Apps (IEEE S&P 2022) 155
D.2 Cybercafes (IEEE S&P 2023) 159
D.3 Security and Privacy Advice in the Majority World (IEEE S&P 2026) 162

List of Figures

3.1 Loan Procurement Process for Mobile Loan Apps. 24

3.2 Tala Loan Procurement Process. 25

3.3 Permissions Required by the Two Most Common Mobile Loan Apps in Kenya. 28

4.1 Customers at Different Cybercafes Located in Nairobi, Kenya, in July 2022. . 54

5.1 Top Advice for Staying Safe Online. 94

D.1 Email Containing a Right To Publish Statement. 155

D.2 Email Containing a Right To Publish Statement. 156

D.3 Email Containing a Right To Publish Statement. 159

D.4 Email Containing a Right To Publish Statement. 159

D.5 Email Containing a Right To Publish Statement. 162

D.6 Email Containing a Right To Publish Statement. 162

D.7 Email Containing a Right To Publish Statement. 163

D.8 Email Containing a Right To Publish Statement. 163

D.9 Email Containing a Right To Publish Statement. 164

D.10 Email Containing a Right To Publish Statement. 164

D.11 Email Containing a Right To Publish Statement. 165

D.12 Email Containing a Right To Publish Statement. 165

D.13 Email Containing a Right To Publish Statement. 166

D.14 Email Containing a Right To Publish Statement. 166

D.15 Email Containing a Right To Publish Statement. 167

D.16 Email Containing a Right To Publish Statement. 167

D.17 Email Containing a Right To Publish Statement. 168

D.18 Email Containing a Right To Publish Statement. 168

D.19 Email Containing a Right To Publish Statement. 169

D.20 Email Containing a Right To Publish Statement. 169

List of Tables

3.1 Common Mobile Loan Apps in Kenya. 26

3.2 Permissions Required by Common Loan Apps. 27

3.3 Demographics Table of Loan App Users. 29

3.4 Permissions' Use by Mobile Loan Apps. 37

3.5 Concerning Permissions of Loan Apps. 41

3.6 Non-Concerning Permissions of Loan Apps. 42

4.1 Demographics of Cybercafe Managers. 57

4.2 Demographics of Cybercafe Customers. 58

4.3 Cybercafe Managers' and Customers' Top Three Advice for Staying Safe Online. 81

5.1 Factors That We Considered in Selecting the Nine Majority World Countries. 87

5.2 Demographics of the Local Experts in the Nine Majority World Countries. . 89

Chapter 1: Introduction

In an increasingly digital world, online threats pose a growing risk to individuals and organizations, leading to financial losses [75], reputational damage, and privacy violations [95,186]. In response, experts recommend several strategies for users to protect themselves, including using strong passwords across accounts [23, 71] as well as using tools such as password managers to improve password hygiene [94, 117]. Yet, most of these solutions are developed in Western contexts [61,89] and can fail in other regions in the majority world[1] with different cultures and practices [136], potentially leaving users at risk. **To improve the security and privacy of diverse users in the majority world, this dissertation explores the security and privacy practices, challenges, and needs of various majority world populations.**

Improving the security and privacy of users in the majority world is important for several reasons. First, these countries comprise a majority of the global population, meaning that improving their digital safety can have widespread impact. Second, many majority world countries have relatively lower GDPs per capita compared to Western countries [182], and socioeconomic factors can shape users' security and privacy perceptions and practices. Studying practices in these countries offers valuable insights into how economic constraints shape security behaviors, factors that may otherwise be overlooked in research focused on high-income countries. Third, governments in the majority world are rapidly digitizing public services. While beneficial, this introduces security and privacy risks due to the vast amount of personal information users share via these systems. Further, low digital literacy and limited access to personal devices (which are more pronounced in the majority world) exacerbate security and privacy risks for users. Understanding these challenges is critical for designing inclusive security and privacy solutions that account for a variety of user needs.

[1]The majority world refers to the countries that contain the majority of the world's population, and has been proposed to describe countries located for example in Africa, Asia, and South America. It's an alternative to terms like "underdeveloped," "developing," and "third world" which are pejorative and offensive.

Accordingly, this dissertation investigates security and privacy practices and challenges in the majority world. I begin by investigating mobile loan apps in Kenya, exploring the privacy concerns and tradeoffs users make when using these apps. Next, I broaden my scope to cybercafes in Kenya, highlighting the security and privacy challenges and tensions that users navigate in these shared facilities. Finally, I extend my scope even further to security and privacy concerns and advice across nine diverse majority world countries.

1.1 Research Questions

To investigate security and privacy perceptions, challenges, and practices of users in the majority world, I formulated three research questions. The first two questions focus on two important contexts in Kenya, i.e., mobile loan apps and cybercafes, while the last question expands the scope to broader challenges in nine majority world countries.

RQ1: **What are users' security and privacy concerns, tradeoffs, and behavior when using mobile loan applications?**

I explore why loan app users in Kenya use these apps, and their privacy concerns and tradeoffs with these apps. I also review their phone permissions and privacy policies to understand what data they collect and how they describe using this data.

RQ2: **What are the security and privacy practices, challenges, and advice at shared cybercafe facilities?**

I investigate security and privacy concerns and challenges for customers at cybercafes. I also explore the advice and support that is subsequently offered to customers as well as its impact on their digital security and privacy at the cafes and beyond.

RQ3: **What security and privacy concerns and advice are prioritized by "local experts" across nine majority world countries?**

Lastly, I explore the security and privacy concerns and advice that "local experts" — including cybercafe operators and owners, tech repair shop owners, teachers,

computer and phone sellers — from nine majority world countries prioritize when supporting their constituents. I additionally investigate the contextual factors that influence both the security and privacy concerns and advice that is prioritized.

1.2 Overview of Key Results and Takeaways

This dissertation contributes several insights into the security and privacy practices and needs in the majority world. In the first study on mobile loan apps in Kenya, I find that these apps fill a crucial financial gap in the majority world by offering small loans to many users that would otherwise struggle to procure loans from traditional financial institutions such as banks due to a lack of formal credit history. At the same time, these apps collect a significant amount of sensitive user information including users' SMS and contacts via phone permissions, data that they unfortunately routinely misuse. Despite having a lot of privacy concerns, many users of these apps overlook these concerns as they are more motivated to obtain loans. This work demonstrates that calls for more transparency around data collection by mobile apps that have been recommended in Western contexts [87] may not suffice for loan app users in the majority world. Instead, I argue that stricter policy and application market-level changes are required to adequately protect these users' privacy.

In the second study on cybercafes, I demonstrate the important role that cybercafes play in enabling access to crucial government services that have recently been digitized in Kenya. At the same time, many customers face significant challenges at these facilities, with many not knowing how to use computers and regularly forgetting their passwords. In response, many cybercafe managers advise their customers to use memorable passwords such as their names or national identity card numbers, with one manager even using the same password for all customers. This can severely put their customers' security and privacy at risk. I argue for alternative authentication mechanisms, including password-less authentication as well as the need to explore security and privacy advice in majority world contexts.

Accordingly, my final study investigates security and privacy concerns and advice across

nine majority world countries through interviews with a diverse set of local experts. Local experts detailed several concerns for themselves and their constituents, including fears about account compromise, misuse of personal information, financial scams, among others. Yet, most of the advice that is prioritized by local experts is aimed at protecting users against account compromise, potentially leaving them vulnerable to other risks. Further, while the advice that local experts provide to their constituents is mostly similar to the advice for their own security and privacy as well as advice from the West, local experts tailor their security and privacy advice to the practical needs of their constituents, prioritizing usability, account access, and affordability over strict adherence to what may be considered security best practices. However, majority world users face significant barriers in implementing advice, including not knowing benefits of the advice (e.g., no visible UI changes after security updates), economic constraints (e.g., inability to afford expensive authentic software), and social friction caused by taking protective security and privacy measures such as using an unlock PIN or password on a mobile phone. I make several recommendations, including the need for more consideration of majority world users in technology research and design.

In the remainder of this chapter, I provide a more detailed summary of the three projects that comprise this dissertation, including methods, key findings, and main takeaways. While I led all these projects, I mostly use "we" to reflect the collaborative nature of this work.

1.3 User Concerns with Mobile Loan Apps in Kenya

Access to financial services is crucial and has been promoted by the United Nations as fundamental in eradicating poverty and achieving the Sustainable Development Goals [162]. However, according to the World Bank [43], about 1.7 billion adults in the world remain unbanked with no access to the services of a bank or similar financial institutions. The largest proportions of unbanked populations are often in the majority world e.g. in Africa, where more than 50 % of the population still lacks access to banking services [170].

While mobile money solutions (services that allow users to send and receive money [74]

on their cell phones) have improved financial inclusion, particularly in Sub-Saharan Africa, mobile loan apps have emerged as an easy and straightforward way for many users to access credit as smartphone usage soars in the region [4]. Kenya, particularly, has been one of the majority world countries with widespread usage of these apps due to the success of mobile money services [57, 74] that facilitate quick disbursement of these loans to users. However, these apps collect significant sensitive data from users for example contacts and SMS, with reports indicating they routinely misuse this data [82, 108, 133]. **In this study, we thus investigate why mobile loan app users in Kenya choose to use these apps, as well as the privacy concerns and tradeoffs they navigate when using these apps.**

To investigate loan apps, we conducted semi-structured interviews ($n = 20$) with mobile loan app users in Kenya. As part of these interviews, participants reviewed the permissions used by their loan apps and described how they perceived these permissions to be used, and any concerns they had with access to this data. We additionally reviewed the privacy policies of these apps to learn how they indicated using and securing users' data.

I present the findings of this study in chapter 3. While loan apps fill a crucial financial gap in the majority world by providing small loans to users, many of whom lack a formal credit history, we also find that these apps collect significant sensitive data from users via permissions. This includes users' contacts and SMS. However, these apps not only fail to transparently disclose how this sensitive user data is used via their privacy policies, but also routinely seem to misuse this data, for example by calling participants' contacts when they default in repayment as detailed by several participants in the study. This is in spite of these apps not informing users they will use their data this way. Despite their privacy concerns, however, many users overlook these concerns to procure loans with the apps.

We offer recommendations to regulators, application markets, developers, and the research community to protect users of mobile loan apps in the majority world. We argue that local regulators should consider enacting privacy laws to protect users of these apps. Mobile loan apps, on the other hand, need to transparently and accurately inform users how

they collect, use, and secure their data, perhaps through updates to their privacy policies. App markets should regularly check user reviews on their platforms with the goal of removing apps that are malicious or invade users' privacy while other researchers can further analyze the apps we have identified to determine if they adequately secure users' data.

1.4 Security and Privacy Challenges and Practices at Cybercafes in Kenya

Besides making many people turn to loan apps for credit, financial adversity coupled with the recent digitization of government services has made many people in Kenya to increasingly turn to cybercafes to access essential services. However, many of the cafe users may have never used a computer before and likely face significant usability and security challenges at these facilities, including general computer usage, online account creation, and password management. **Accordingly, this study explores challenges, particularly related to security and privacy, that customers encounter at cybercafes, followed by the security and privacy advice and support they receive from cybercafe managers.**

To investigate cybercafes, we conducted $n = 36$ semi-structured interviews at cybercafes in Kenya: $n = 14$ with managers and $n = 22$ with customers. We asked both the managers and customers about services they mostly provide or seek at the cybercafes respectively, challenges customers encounter, and the advice and support that managers offer to them.

I present the results of this study in chapter 4. We find that cybercafes play a critical role in the majority world by allowing many people to access printing, government, and other internet services. At the same time, customers experience significant usability and security challenges around general computer usage, online account creation, access, and recovery. Many customers rely on cybercafe managers when navigating these challenges, with many managers selecting passwords for customers that are easy for the customer (and the manager) to remember, such as customers' national ID numbers or names. Unfortunately, this significantly exposes these accounts to password stuffing and guessing attacks.

We offer several recommendations, including the need to consider the needs of diverse

user groups in the majority world, rather than designing all security and privacy solutions for Western audiences. We additionally show how existing security and privacy solutions such as password managers could be helpful in addressing password management challenges, but can fail because of device-sharing practices that remain common in the majority world.

1.5 Security and Privacy Advice in the Majority World

Our work on cybercafes in Kenya [103] as well as other prior work [125, 126] show how security and privacy advice plays a critical role in how users stay safe online. While there has been prior work investigating the sources and efficacy of security and privacy advice [50, 125, 128, 129], this work has primarily focused on the US, despite other work finding that internet users outside the West have unique needs, threat models, and practices due to different cultures [136], infrastructure [103], and socioeconomic backgrounds [102, 126]. Thus, we cannot simply rely on security and privacy advice curated and evaluated in the West to generalize to the rest of the majority world. Given that prior work in the majority world [67, 103] finds that people often rely on "local experts" — i.e., individuals that provide tech assistance or advice to others in their community e.g., cybercafe operators, phone sellers, tech repair shop owners — for advice on online safety, **this study aims to investigate both the concerns, and security and privacy advice that local experts across the majority world prioritize when advising their constituents to stay safe online.**

To investigate security and privacy concerns and advice in the majority world, we conducted 70 semi-structured interviews with local experts in a variety of occupations, e.g., cybercafe operators, tech repair shop owners, teachers, and computer and phone sellers. The local experts we interviewed are from nine majority world countries in four continents: Africa (Ghana, Kenya, and Nigeria), Latin America (Brazil and Mexico), Asia (China, India, and Pakistan), and the Middle East (Türkiye). These nine countries account for close to 50% of the world's population [181], and are diverse in their locations, internet penetration rates, smartphone ownership rates, internet freedom, cultures, religion, and gender (in)equality.

I present the results of this study in chapter 5. Local experts detailed several concerns for themselves and their constituents, including fears about account compromise, misuse of personal information, financial scams, among others, with these concerns exacerbated by factors including cultural norms and financial constraints in the majority world. Yet, most of the advice that is prioritized by local experts (including the use of strong passwords and two-factor authentication) is aimed at protecting against account compromise, potentially leaving users vulnerable to the other risks. Further, we surface advice prioritization challenges in the majority world due to the broad range of security and privacy advice offered.

While the advice that local experts provide to their constituents mostly matches the advice they prioritize for their own security and privacy, we find some differences. For instance, while local experts use VPNs, they advise their constituents to use trusted experts and memorable passwords. When we compare local experts' advice to advice from the West, we find significant overlap but with differences. For example, password managers and regular software updates are frequently encouraged in the West, but less so by local experts in our study. Importantly, users face significant barriers in implementing advice, including not knowing benefits (e.g., no visible UI changes after security updates), economic constraints (e.g., inability to afford authentic software), and social frictions that are caused by taking protective measures such as using an unlock PIN or password on a mobile phone.

While prior work has quantified correlations between sociodemographic factors and security and privacy practices [174], our study contributes in-depth insights into how contextual factors such as gender, culture, and religion shape security and privacy concerns and advice in the majority world. For instance, collectivist cultures and religion may compel people to share their devices, undermining privacy affordances from the West where device sharing is less common. Gender influences advice-seeking behaviors, with women preferring to seek advice from other women. Our work suggests the need for better advice prioritization and consideration of majority world users in tech and security and privacy design. We also advocate for better translation of tech tools and security and privacy advice.

1.6 Organization

The rest of this dissertation is organized as follows: In chapter 2, I discuss prior work on Android permissions, digital lenders, cybercafes, security and privacy advice, cross-national security and privacy research, and undeserved populations in security and privacy. In chapter 3, I present our work on privacy concerns and tradeoffs when using loan apps in Kenya. In chapter 4, I expand the scope to cybercafes in Kenya, and in particular security and privacy challenges and concerns people navigate when using these facilities. In chapter 5, I expand the scope even further beyond Kenya, investigating security and privacy concerns and advice across nine countries in the majority world. In chapter 6, I summarize major findings from this dissertation and conclude with promising directions for future research.

Chapter 2: Related Work

In this section, I first discuss prior research on Android phone permissions and digital lenders, providing context for our investigation of mobile loan apps in Kenya. I then expand the scope to shared digital access spaces, such as cybercafes and public libraries, where security and privacy challenges emerge due to device and resource sharing. Finally, I broaden the scope further to explore security and privacy advice more generally, noting how much of the existing research has centered on Western populations. I also highlight comparative studies between Western and majority world contexts, demonstrating how security and privacy solutions designed with Western assumptions often fail to account for the realities and needs of users in the rest of the world, sometimes leaving users at risk.

2.1 Android Phone Permissions

Android permissions allow users to control information that can be accessed on their devices by mobile applications [1, 44]. This could be reading data on the device such as contacts and SMS, all the way to accessing hardware features such as the device's camera or microphone. Android categorizes permissions into three broad categories, install-time, run-time, and special permissions. Install-time permissions give an application access to less sensitive data and are automatically granted to the application when it is installed. Run-time permissions, also known as dangerous permissions, give access to more sensitive user data, and require explicit user approval [1, 155] before they can access the user's information. Special permissions, on the other hand, correspond to specific application operations and can only be defined by the Android platform itself. Throughout our study on mobile loan applications presented in chapter 3, we focus on run-time permissions as these permissions access sensitive data and require direct user approval before they can access users' data.

Prior work has explored user understanding of Android permissions. Through a usability

study, Felt et al. [45] found that most users pay less attention to permission warnings in addition to not properly understanding how different permissions are used. Kelley et al. [79] confirmed these results, finding that users generally view and read Android permissions, but do not understand them. They additionally found that users are unaware of the security risks posed by mobile applications due to overly trusting the application markets. Despite several improvements [1] to Android since then, our loan apps study similarly finds that users struggle to understand the use of some permissions, notably their telephone and storage. Our study is also the first to show user comprehension of permissions in Kenya.

Users' willingness to grant and deny permissions to mobile apps has also been explored, with Jialiu et al. [88] finding that users' inclination to grant a given permission to a mobile application is strongly influenced by the purpose associated with such a permission. This is also reflected in our loan apps study whereby users are unconcerned about access to permissions they believe are legitimately required by the mobile loan application. Other studies have explored the permissions required by Android applications. Khatoon et al. [81] studied the different ways in which applications gain access to sensitive device permissions when installed on Android, finding that many free apps tend to request unnecessary permissions to gather valuable user data. Chia et al. [26] found that free apps request more permissions than is typical across Facebook applications, Chrome extensions, and Android applications. Additionally, they found that popular applications request more permissions than average. Our loan apps study observes a similar phenomenon with common mobile loan applications in Kenya, with these apps collecting significant sensitive user data via permissions to verify and calculate users' credit worthiness when offering them loans.

Tools have been developed to check if mobile applications use the permissions they require. Felt et al. [44] built a tool called Stowaway to detect if Android applications require more permissions than they actually need, establishing that about a third of the applications they studied were over-privileged. Interestingly, they found evidence that developers were trying to follow the least privilege approach but occasionally fail due to insufficient

documentation. Johnson et al. [76] developed an architecture to map Application Programming Interface (API) calls of Android applications to their required permission(s), finding that most application developers do not use correct permission sets for their applications. This often leads to either over- or under-privileged applications. Additional tools have been developed to enable users make better privacy decisions. Liu et al. [90] developed a personalized privacy assistant for mobile app permissions and found that not only were their recommendations followed by users but also spurred them to review and modify their permission settings using daily nudges. Kelley et al. [80] found that by bringing privacy information to users when they are making decisions, users can be assisted in choosing apps that request fewer permissions. Wijesekera et al. [178, 179] and Tsai et al. [156] have recently shown that users' decisions regarding the granting or denial of permissions are contextual, and that machine learning can be used to assist them to make better decisions.

More recent work on Android permissions has been conducted by Almomani and Khayer [9]. By analyzing Android permissions since Android's inception in 2008 to 2020, they find that permission categories have been continuously increasing on the Android platform. This is also reflected in Android applications, with several applications increasing their permission usage by over 70 %. Despite several design improvements to the Android Operating System [1], Almomani and Khayer still find over-privilege as a persistent challenge with most Android applications, consistent with our findings on common mobile loan apps in Kenya which request for significant sensitive data from users via permissions.

2.2 Mobile Loan Apps and Other Digital Lenders

Our study on mobile loan apps presented in chapter 3 is most closely related to the research conducted around online credit lenders [20] and mobile money services [19, 123] by Bowers et al. and Reaves et al. Through a comprehensive security analysis of emerging online credit lenders around the world, Bowers et al. [20] found that these applications collect previously undisclosed data types as well as insecurely handle this data. Bowers et al. further found that

these applications' privacy policies are not only hard to read, but do not mention all data that is collected from users. Through another study, Bowers et al. [19] studied privacy policies of mobile money services. Unlike the online credit lenders, they found that almost half of mobile money services do not have a privacy policy. For apps with existing policies, they similarly found that these policies are either too hard to read for their target audiences or clearly fail to show what user information is collected and how it is stored. Through a related study, Reaves et al. [123] uncovered multiple vulnerabilities with Android mobile money applications, including information leakage that can allow attackers to modify transactions and even steal funds. Our study on mobile loan apps in Kenya confirms and expands on these findings. Unlike Bowers et al. and Reaves et al., we leverage a user-centric approach through semi-structured interviews with users of these applications to show, for the first time, user concerns, tradeoffs and behavior when using mobile loan applications in the majority world. We also briefly review their privacy policies and the permissions they require to contextualize participants' sentiments. While we find that these apps are useful for many users facing economic challenges and without formal credit history in the majority world, we also show how these apps raise many privacy concerns and discuss ways in which law makers and application markets can hold them more accountable.

2.3 Cybercafes and Public Libraries

While mobile loan apps pose individual privacy risks for users, we now discuss how sharing of digital spaces such as cybercafes and public libraries introduce security and privacy risks for users. Cybercafes in particular have not received much attention in the research community of late. However, earlier studies investigated the role of cybercafes, as well as characteristics of customers and their usage patterns in different regions and countries. Through street surveys, Gitta and Ikoja-Odongo [53] demonstrated how cybercafes were enabling Ugandans to access information in 2003, and Haseloff [62] found that cybercafes were the most-commonly used means to access the Internet in Bangalore, India in

2005. Haseloff further found that most cafe customers tended to be younger and able to communicate in English while another study in the Philippines in 2012 found that most cybercafe customers were men [22]. Public access venues, such as telecenters, libraries, and cybercafes, are fundamental in enabling communities access the Internet in Colombia [54].

Most closely related to our cybercafes work presented in chapter 4 are four studies that investigated security and privacy practices at cybercafes in Morocco [69] and public libraries in the US [37, 91, 98]. Through a field study complemented by questionnaires for both cybercafe managers and customers in Morocco, Houmz et al. [69] found that managers were hesitant to update the cybercafe computers' operating systems because of limited resources on the devices, a theme also noted in our study of cybercafes in Kenya. The study further found that an alarming 60% of the cybercafe computers were infected with malware. Recently, Dooley et al. [37], Luo and Warford et al. [91], and McDonald et al. [98] have conducted interviews with IT professionals working in public libraries in the US, exposing challenges and constraints to privacy and security practices at these facilities. Different from these studies, we use semi-structured interviews with Kenyan cybercafe managers and customers to investigate cybercafe practices and behaviour, as well security and privacy advice offered to customers. We also investigate advice that users in Kenya consider important for staying safe online and compare our findings to prior work [23, 71]. We show how security advice from Western contexts breaks down at these facilities, with managers instead advising their customers to use memorable passwords such as their names to remember these passwords. This has severe implications on their security and privacy.

2.4 Security and Privacy Advice

Our study at cybercafes in Kenya showed how sharing devices can complicate users' security and privacy. We now discuss previous work on security and privacy advice, and show how this advice might be impractical in the majority world for example because of device-sharing.

Security and privacy advice has particularly been the subject of much research in the

community. Through two online surveys in the US with expert and non-expert users in 2015, Ion et al. [71] noted differences between what experts and non-experts consider important for staying safe online, with experts recommending OS updates, strong passwords, and two-factor authentication. In contrast, non-experts indicated that using anti-virus software, strong as well as constantly-updated passwords were more important. Through a replication study with European participants, Busse et al. [23] confirmed most of these findings in 2019. An even more recent replication of Ion et al.'s study by Ortloff [114] in 2025 notes that both experts and non-experts are beginning to particularly focus on authentication practices such as two-factor authentication, while the use of anti-virus is becoming less popular. In our study with cybercafe managers and customers in Kenya, we find that most participants consider logging out of their accounts, strong passwords, avoiding clicking on suspicious links, and not saving passwords in the browser as the most important advice for staying safe online. The differences with previous work can be attributed to different ways in which people access the Internet in different places, suggesting that security and privacy advice is only effective if it considers the specific needs of the target population.

Researchers have also investigated the sources of security and privacy advice as well as its efficacy, comprehensibility, and actionability. By identifying search queries for advice on the web with crowd workers from MTurk followed by user studies with experts and non-expert users in the US, Redmiles et al. [128] found that users perceive most security imperatives as fairly actionable but struggle to prioritize, similar to Reeder et al.'s findings [129]. The study suggests the identification of a minimal set of highest impact and most practical advice to help end-users. Through a census-representative survey in the United States, Redmiles et al. [125] also found that socioeconomic status influences advice sources for users, with the socioeconomically advantaged more likely to take advice from their workplaces while those with lower skills rely on family and friends. Other research has identified factors that influence advice sources and adherence, including the trustworthiness of advice [127], convenience/security trade-offs [7,41], and socio-demographic factors [30,72,125,126,172].

Some of these results, including trustworthiness of the source of advice, are confirmed in our study of security and privacy advice in the majority world.

Social media has also proven to be a useful source of security and privacy advice. During the Black Lives Matter protests across the US in 2020, Boyd et al. [21] were able to identify various classes of security and privacy advice for protesters through Twitter and Google searches. By analyzing security and privacy advice on Twitter during the Russian invasion of Ukraine in 2022, Schmüser et al. [140] found that prioritization of advice remained a persistent challenge, similar to prior work [128, 129] while Wei et al. [175] have recently shown how "anti-security" and "anti-privacy" advice on TikTok unfortunately enables surveillance and control in interpersonal relationships. TikTok has additionally been shown to facilitate cheating on proctored tests [144]. Contrastingly, Bhagavatula et al. [16] have found that user interactions with security advice on Twitter and Facebook are scarce.

2.5 Cross-National Security and Privacy Studies

As security and privacy needs, challenges, and behaviors vary across countries and cultures [15, 27, 66, 73, 139, 141], some researchers have started to explicitly compare practices across countries and contexts to design more inclusive solutions. In a qualitative study with 24 participants in five majority world countries i.e., the Philippines, Brazil, India, Egypt, and Nigeria ($n = 120$), Umbach et al. [161] found that device-sharing practices common among many participants often result in consistent concerns about privacy. Other cross-national studies have shown pronounced differences in security and privacy perceptions and practices between Western countries versus majority world countries. In the case of digital contact-tracing, for instance, participants in the West tend to have more privacy concerns compared to their majority world counterparts [142]. Some of the reasons for these differences include differences in culture, technology infrastructure, context, laws, location, religion, gender (in)equality [31, 103, 124, 126, 169] among others. Our cross-national study across nine majority world countries presented in chapter 5 highlights how factors including financial

constraints and social relations can often dictate security and privacy behaviors, but also prevent people from implementing recommended security and privacy advice.

2.6 Security and Privacy in the Majority World

One of the main contributions of this dissertation is highlighting the unique security and privacy needs of majority world populations which remain underserved in existing work. This work joins a growing number of studies that have recently started to investigate these users. For instance, our work on loan apps in chapter 3 [102], and two recent studies [84,122] show how financial adversity often compels loan app users in Kenya and India to overlook their privacy concerns with these apps to procure loans. Kotut [84] shows how laxity in policy enforcement leaves loan app users in Kenya vulnerable to these apps. This suggests the need for stronger policy and platform changes to better protect these users' privacy.

In South Africa [130] and Kenya [105], users of social messaging apps such as WhatsApp are more concerned about interpersonal privacy than the security and privacy risks posed by the platforms themselves; this explains the proliferation of WhatsApp mods in Africa despite their security risks [105]. In South Asian countries including India, Pakistan, and Bangladesh, women are culturally expected to share their phones with other people in the household [136]. However, this makes it very challenging for them to protect their privacy on these devices, forcing many to resort to content deletion and the use of app locks.

In Lebanon and Ghana, failing infrastructure necessitates "infrastructuring" practices to overcome institutional and systemic failures [97, 160]. For instance, users rely on intermediaries to charge their devices when they lack access to electricity. As infrastructuring poses security and privacy risks to users, McClearn et al. [97] introduce the concept of "security patchworking" to describe practices that users adopt to protect their security. Similar infrastructuring and patchworking practices have been noted in the majority world and beyond, e.g., among refugees [70,134], activists [34], migrants [29], domestic workers [147], LGBTQ+ users [77], women [17,152,176], and low socioeconomic users [18,63,83,103].

Accordingly, researchers have started to design security and privacy solutions that are more tailored to the needs and constraints of the majority world, including mHealth solutions designed to aid frontline health workers in India, Kenya, and Zimbabwe [86], redesigned privacy-preserving protocols for mobile money services in Kenya [148], and affordable contact-tracing wearables suitable to low and middle income countries [135].

Additional research has shown that many majority world users rely on others [67] for security and privacy advice due to collectivist cultures compared to their Western counterparts from individualistic cultures [124]. For instance, many low-income users and older adults in India [107, 137] and Bangladesh [6, 151] rely on other more skilled users (e.g., from their families) to access technology, otherwise known as inter-mediated technology usage. In Kenya, many users rely on cybercafe managers for technology access but also security and privacy advice [103]. At the same time, the support and advice offered by non-traditional experts can have profound impact on users' digital safety. For instance, cybercafe managers in Kenya often advise customers to use simple passwords such as their national identity card numbers and their names, putting them at-risk [103]. This dissertation calls for more research into the security and privacy practices of users in the underserved majority world in order to design security and privacy solutions that protect all users.

Chapter 3: Security and Privacy Concerns with Mobile Loan Apps in Kenya

This chapter details our research on privacy concerns and tradeoffs with mobile loan apps in Kenya. Mobile loan apps have become increasingly popular in Kenya, offering loans to many users that would otherwise struggle to procure loans from traditional financial institutions such as banks due to a lack of formal credit history. However, these apps collect significant user data that they sometimes misuse. To investigate concerns with these apps, we conducted semi-structured interviews with 20 mobile loan app users in Kenya. We additionally reviewed the data collection practices of common mobile loan apps.

We find that loan apps in Kenya are permissioned to collect a lot of sensitive user data, including users' contacts, which they seem to routinely misuse. For example, when users default, their contacts are threatened, despite these apps not informing users that their data will be used this way. While most users of these apps have privacy concerns, they overlook these concerns as they are more motivated to procure loans. We offer recommendations to regulators, app markets, and the research community that can protect users of these apps.

This chapter is based on work originally published at the 43rd IEEE Symposium on Security and Privacy [102]. I have permission from my coauthors and publishers to use this work in my dissertation. Copies of all copyright permissions are in Appendix D.1.

- Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In Proceedings of the 43rd IEEE Symposium on Security and Privacy, Pages 2304-2319, San Francisco, CA, USA. May 2022 [102].

I came up with the idea for this project, designed the interview protocol, performed initial pilots, collected the data, analyzed it, and wrote the paper. Darika Shaibekova assisted with secondary qualitative coding. My co-authors provided a lot of feedback throughout the research process, from ideation all the way to writing the manuscript.

3.1 Introduction

Access to financial services is crucial for economic growth and has been promoted by the United Nations as fundamental in eradicating poverty and achieving the Sustainable Development Goals [162]. However, according to the World Bank [43], about 1.7 billion adults in the world remain unbanked with no access to a bank or similar financial institutions. The largest proportions of unbanked populations are in majority world economies such as in Africa, where more than 50 % of the population lacks access to banking services [170].

While mobile money solutions (services that allow users to send and receive money on their cell phones [74]) have improved financial inclusion, particularly in Sub-Saharan Africa, mobile loan apps have emerged as an easy and straightforward way for many users to access credit as smartphone usage soars in the region [4]. Claiming to improve "financial inclusion" in these communities [2, 42, 57, 64], mobile loan applications allow users (many without formal credit history) to easily and quickly access loans on their smartphones. These apps do not require collateral or security and solely rely on the self-reported registration information along with data collected from users' smartphones via permissions to offer loans.

Kenya, particularly, has been one of the countries in the majority world that has seen the earliest and perhaps most widespread adoption and usage of mobile loan applications. This has been fueled by the country's huge success of mobile money services such as M-Pesa [57, 74] coupled with growing smartphone adoption [118] that allows users to apply and receive loans from mobile loan applications directly to their mobile phones. Some of the most widely used mobile loan applications such as Tala and Branch began operations in Kenya before diversifying to other majority world countries such as India [42].

As this is a relatively new and therefore unregulated industry, mobile loan applications charge extremely high interest rates and often require repayment within shorter durations of time, compared to traditional financial institutions such as banks. Further, they collect significant sensitive data from users via data available on the mobile device, authorized

through the phone's permission system. This includes collection of contacts and location as part of verifying and calculating users' credit worthiness [2, 57]. Tala, for example, claims to have repayment rates of more than 90 % achieved through modeling users' routine habits by tracking places they regularly visit and people they frequently contact [2].

Despite widely reported privacy concerns [82, 108, 133], most mobile loan applications claim that users have no concerns, with Shivani Siroya, the founder of Tala, saying "customers have no privacy concerns with Tala as they willingly grant access to their private data through the phone permissions for their credit scores to be developed [2]." Nevertheless, the usage, concerns and behavior with mobile loan applications in the majority world remains largely unexplored. Our study is therefore aimed at investigating the reasons for usage and concerns with the emerging mobile loan applications in the majority world, specifically in Kenya. We were also motivated to study user understanding and misconceptions with security and privacy and how this influences their usage of these loan apps. We seek to answer the following three research questions in this study:

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

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

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

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

each permission, followed by concerns and non-concerns with loan apps' access to these permissions. Lastly, participants shared any other information they had about loan apps.

Mobile loan apps are widely used in Kenya, and our results indicate that they fill a crucial financial gap in the majority world by offering loans to users that otherwise have no formal credit history or collateral. In fact, Tala and Branch, the two most common mobile loan apps, have over 5 and 10 million downloads respectively on Android's Google Play alone. At the same time, we find that common mobile loan apps are permissioned to collect significant sensitive user data, similar to other digital credit lenders [20] previously studied. Each of the eight most common loan apps we explored requires access to users' contacts, SMS, location, and storage, while seven require access to users' telephone. While users seem to understand what some of these permissions are used for by these apps, they mostly do not know or misunderstand what most of the permissions are used for, confirming prior work on general comprehension of Android permissions [45, 79].

Contrary to what mobile loan apps postulate [2], an overwhelming majority of users have concerns with loan apps, particularly regarding their privacy. Most participants are particularly worried about these apps' access to their contacts, citing that some of these apps call their contacts when they default in loan repayment; this is in spite of these apps not indicating they will use users' data this way. Participants are also concerned about the high interest rates coupled with short repayment periods offered by mobile loan apps. However, they often overlook these concerns as this outweighs their need to procure the loans.

Our work offers recommendations to regulators, application markets, developers and the research community to protect users of mobile loan apps in the majority world. Local regulators should consider enacting laws, similar to those used to regulate other financial players, to prevent user exploitation for example through high interest rates. Mobile loan apps, on the other hand, need to transparently and accurately inform users how they collect, use, and secure their data, perhaps through updates to their privacy policies. App markets should regularly check user reviews on their platforms with the goal of removing apps that

are malicious or invade users' privacy while other researchers can analyze the applications we have identified to determine if they adequately secure users' data.

3.2 Background on Mobile Loan Apps

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

3.2.1 About Mobile Loan Apps

Mobile loan apps are applications that users download from Android's Google Play, Apple's App Store, or third-party markets to procure loans. Unlike mobile money services, such as M-Pesa, that allow users to conduct financial transactions on their cell phones [74] for example purchasing goods, paying bills, sending or receiving money, mobile loan apps are solely used to procure loans. Further, they calculate credit scores based on information such as location, contacts, or SMS gathered from the prospective borrower's phone [2, 57] through phone permissions. As smartphone usage grows in majority world countries [4] such as Kenya [118], these apps have become extremely common due to their speed in disbursing small loans to users coupled with the minimal paperwork or security they require to offer these loans. This is in stark contrast to traditional financial institutions such as banks that require formal credit history or collateral to offer similar loans.

Most mobile loan apps are startups with huge investments from venture capitalists [57] and claim that they are primarily motivated to boost "financial inclusion" in the majority world where most people remain unbanked and lack formal credit history [2, 42, 57, 64]. Tala, one of the earliest and most common mobile loan apps in Kenya, claims it had lent over $1 billion dollars to more than four million customers spread across three different continents by 2019 [64]. Branch, another common loan app, had over three million customers as well

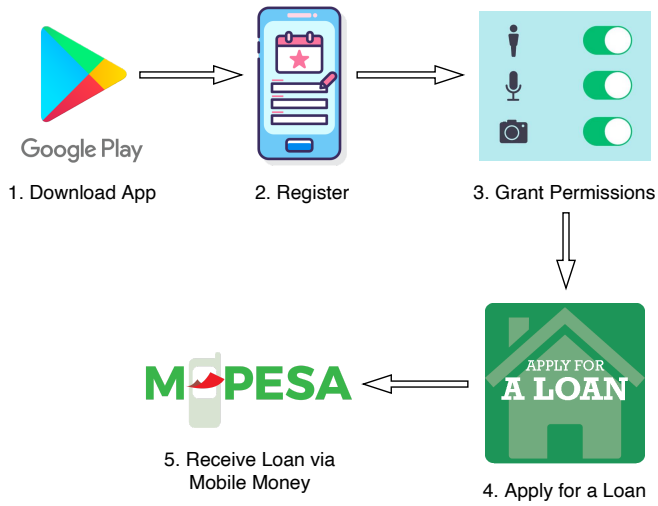


Figure 3.1: Loan Procurement Process for Mobile Loan Apps.

as over 15 million loans issued to customers in Kenya, Nigeria, Tanzania, Mexico, and India by 2019 [57]. According to the Kenya Credit Bureaus, more than 19 million Kenyans (about 37% of the population) had used a mobile loan application to borrow money by 2019 [32].

3.2.2 How Mobile Loan Apps Work

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

After registering and granting access to the required permissions, the user can borrow money up to the limit set by the application, with Tala and Branch granting on average $50 to most borrowers [2, 57]. The borrowing process is usually fast, with the money directly disbursed to the user's phone through existing mobile money payment services such as M-Pesa [74] in Kenya. According to Tala [2], users can request and receive loans in under two minutes, and become eligible to borrow even higher amounts upon timely

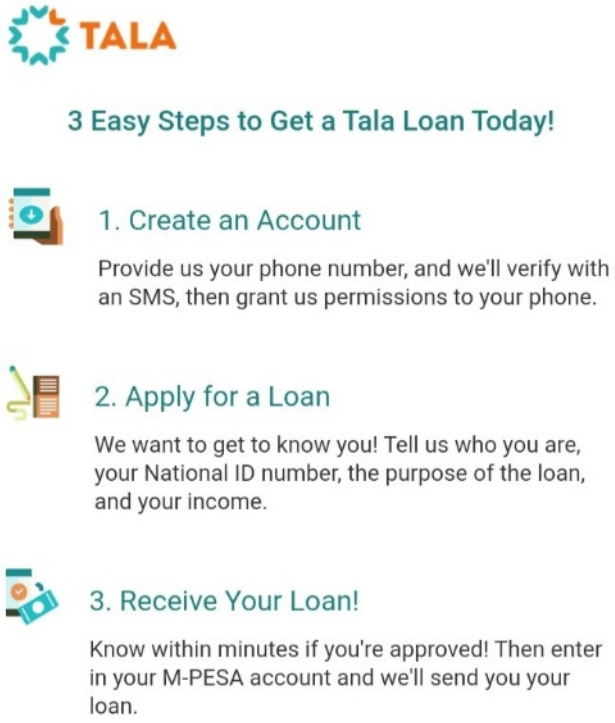


Figure 3.2: Tala Loan Procurement Process.

repayment. Further, Tala claims to have high repayment rates, similar to banks, achieved using credit scoring algorithms that analyze and build models of users' routine habits, including tracking their movement through their smartphones' GPS data [2]. Figure 3.1 shows the loan application process generally, while Figure 3.2 shows the loan application process for Tala once a user has downloaded and installed the loan application.

3.2.3 Common Mobile Loan Apps in Kenya

Kenya is one of the majority countries that has seen the earliest and most widespread usage of emerging mobile loan applications in the world. This is in part due to the huge success of M-Pesa [57, 74], a robust mobile money payment system that allows users to conduct financial transactions on their cell phones [74], as well as growing smartphone adoption in the country [118]. This has attracted several financial technology companies looking to leverage the plethora of user data on smartphones to offer loans to these populations, with a

Table 3.1: Common Mobile Loan Apps in Kenya.

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

majority of these users otherwise ineligible for loans from traditional financial institutions such as banks due to a lack of formal credit history or collateral.

For this study, we consider a mobile loan app to be common if it is used by at least two participants during our interviews and has at least 500 000 downloads on the Google Play. In the end, we had eight common mobile loan apps, with Tala and Branch the most common. These apps are used by more than half of the participants in our study. They additionally have high download numbers on Google Play, with downloads of over 10 million for Branch, and over 5 million for Tala. Other common mobile loan applications are OKash (8), OPesa (5), Zenka (5), Zash (2), iPesa (2) and MoKash (2). This is summarized in Table 3.1.

3.2.4 Permissions Required by Mobile Loan Apps

To assess customers' ability to pay back loans, loan apps require users to provide their personal information via the registration process and grant access to restricted data on their phones via permissions. By checking Android's Google Play, we find that the most common loan apps in Kenya are permissioned such that they can collect significant sensitive data from users. Each of the eight most common loan apps requires access to users' contacts, SMS, location, and storage; seven require access to telephone while four require access to the camera. This has been similarly noted for other emerging digital credit lenders around the world [20] that collect significant, previously undisclosed data types from users.

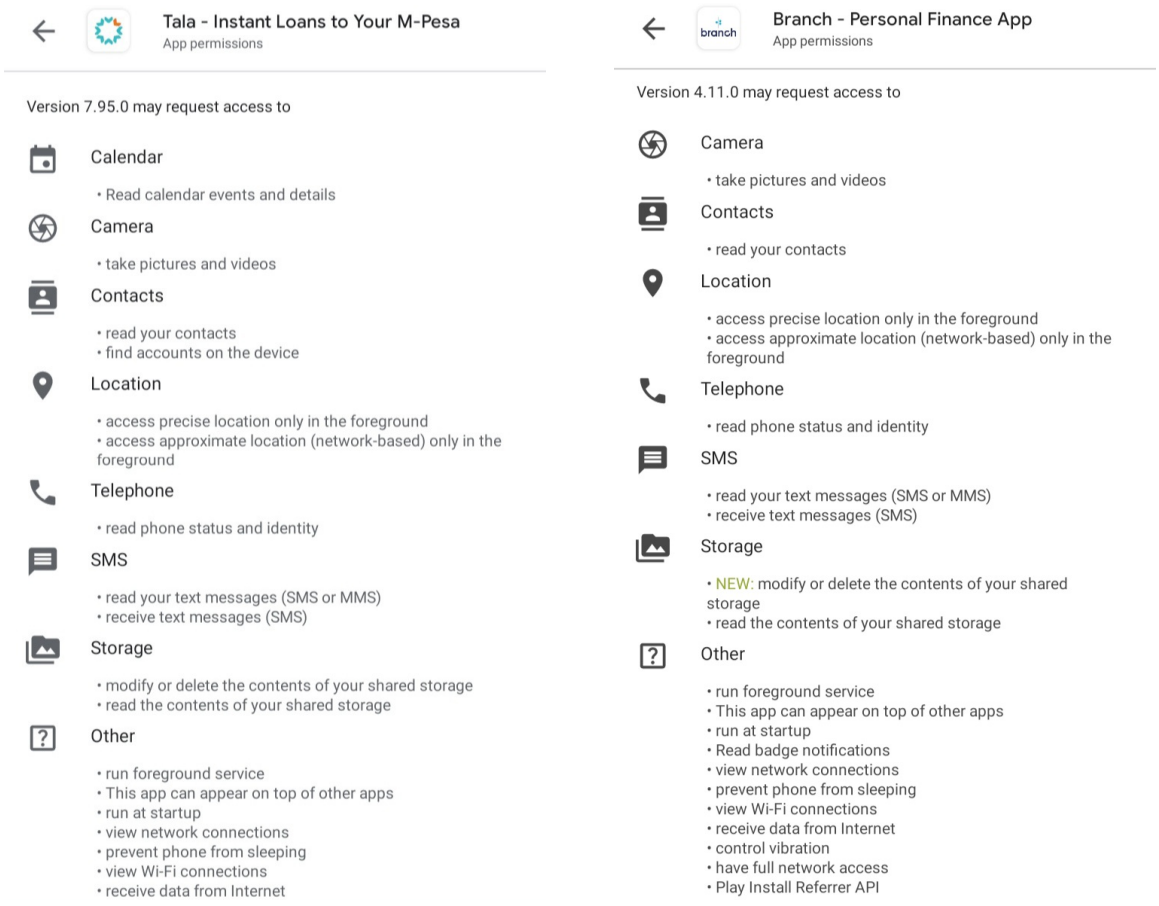
Table 3.2: Permissions Required by Common Loan Apps.

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

These results are summarized in Table 3.2, with Figure 3.3a showing the permissions required by Tala and Figure 3.3b showing permissions required by Branch. Note, we only focus on Android's run-time permissions as these permissions allow access to sensitive user data; therefore, users must explicitly grant these permissions before their private data is accessed [1]. We do not consider install-time permissions, as they access less sensitive data and are automatically granted when an application is installed on the user's smartphone.

3.2.5 Privacy Policies of Mobile Loan Apps

A privacy policy serves to inform users what data is collected from them, the purpose the data is used for, and how long the data is retained for a given product or service [78]. Each of the eight common mobile loan applications used by our participants has a privacy policy, with most of them indicating that they collect information from users via the registration details provided, as well as data extracted through phone permissions to compute users' credit worthiness. However, most of these policies are not conclusive. For instance, some participants complain about their contacts getting contacted when they default in payment; this is inspite of the loan apps not indicating they will use this data in this manner. This is similar to Bowers et al.'s findings on emerging digital credit lenders [20] and mobile money services [19] whereby the privacy policies of these services are not only hard to read but also fail to disclose all data collected from users.



(a) Permissions Required by Tala.

(b) Permissions Required by Branch

Figure 3.3: Permissions Required by the Two Most Common Mobile Loan Apps in Kenya.

3.3 Methodology

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

3.3.1 Recruitment and Demographics

We recruited (n=20) participants by advertising on Twitter, Facebook, and WhatsApp as these platforms are widely used in Kenya. Further, one of the researchers is from Kenya and has a good following on these communication mediums. Snowballing [52] was additionally

Table 3.3: Demographics Table of Loan App Users.

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

used whereby participants recommended other people that had used mobile loan applications in Kenya. We restricted mobile loan apps to applications downloaded from the mobile app stores (specifically Android's Google Play) solely for the purpose of procuring a loan, unlike banking or mobile money applications which offer loans to users in some cases, but not as their primary functionality. After open-coding the transcripts, we found that no new themes emerged after 15 interviews, so we should have reached saturation with 20 participants.

To be eligible for the study, participants had to be at least 18 years old and successfully used a mobile loan application in Kenya. Our participants were mostly young (70 % between 18 – 29), well-educated (85 % had a Bachelor's degree or above) and formally employed (75 %). Table 5.2 provides the full demographic information of our participants.

3.3.2 Interview Procedure

The interview questions were developed around our research questions, seeking to first understand how users perceive permissions as these permissions often provide the gateway to access of sensitive information on their devices. We also took inspiration from prior work [44, 45, 79] on Android permissions, aiming to understand how user understanding of these permissions can influence concerns and behavior when using the apps.

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

For the second part of the interview, participants were asked to indicate the permissions required by the mobile loan app they had most commonly used by referring to the settings menu on their mobile device. Many participants were no longer using the app and had deleted it from their device. For those, they were directed to Android's Google Play to review the permissions for the application from there. Participants were asked to describe each permission, what they believed it was used for, and indicate any concern or non-concern for the application using that permission. Lastly, we asked participants if they would behave differently with respect to mobile loan apps as a result of the interview. All the interviews were audio-recorded and conducted in English, one of Kenya's official languages [113]. The full interview protocol and questions can be found in Section A.1 of the Appendix.

3.3.3 Data Collection

We piloted our interview procedure with two participants and used their feedback to improve the clarity of our interview questions. We used follow-up questions and deeper probing to allow participants to offer more in-depth information [28]. All interviews were conducted during July 2021. During that time, health precautions against the COVID-19 pandemic were in place, and so we conducted interviews remotely using WhatsApp or direct phone calls, depending on the participants' preferences. Each participant was compensated either 2GB worth of internet data or 125 minutes of call time — this was directly sent to the participant's phone number after the interview. The interviews lasted 21 minutes, on average.

3.3.4 Data Analysis

One researcher transcribed and independently coded seven hours of the interview recordings from all participants, developing a primary codebook. To verify its consistency, a secondary coder used this codebook to code half of the interview responses before inter-coder reliability was calculated. Since a good reliability score was not achieved after the first round, the two researchers met to collaboratively update the codebook. After the second round, high agreement [115] ($\kappa > 0.7$) was reached, with the primary codebook used to discuss emerging themes from the study across all the 20 interviews.

3.3.5 Limitations

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

Another limitation is that this study focused on mobile loan app users on Android only. Many of these apps are available on iOS, but due to the prevalence of Android devices in Kenya [92] and the use of permissions, Android provides the best platform for investigation. Future work may explore these applications on other mobile operating systems.

As is typical with interview studies, our recruited sample size was relatively small. However, we performed open-coding on the collected data and noted that no new themes were emerging after 15 interviews. We conducted an additional five interviews, and ultimately ended data collection after 20 interviews due to saturation. Further, our results are primarily qualitative, and the counts provided in the codebook available in Section A.2 of the Appendix only highlight prevalence of common themes. Thus, they should not be interpreted as an attempt to generalize beyond our sample.

Our recruitment sample also skewed mostly young and educated participants. We do not claim our results to be representative of the general population of Kenya. Further, as is typical with interview studies, a possible lack of anonymity may limit the information shared by participants [138]. To this end, we informed participants that their personally-identifying information would not be recorded as part of the interview. Further, conducting the interviews remotely may have helped in alleviating this concern. Lastly, our study was only conducted with participants from Kenya, and additional work is required to study mobile loan applications in other countries and contexts.

3.3.6 Ethical Considerations

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

3.4 Results

In this section, we discuss the reasons for the usage of mobile loan apps in Kenya as well as user understanding of the phone permissions they require, and following, we discuss user concerns, tradeoffs, and behavior when using these apps. We do not report counts, and those provided in Tables 3.4, 3.5, 3.6 only add weight to common themes or highlight unique perspectives. However, they should not be interpreted as an attempt to make generalizations.

3.4.1 Reasons for Use of Mobile Loan Apps

Most participants use loans apps because of their quick loan disbursement coupled with minimal paperwork required compared to traditional financial institutions such as banks. For instance, P12 stated that *"the good thing with Tala and Branch [is that] you get [the] money instantly, it doesn't even take, like, 5 minutes"* while P16 indicated that mobile loan apps require less paperwork and are quick in disbursing loans: *"When you compare [loans from the apps] with bank loans; where you will go to the bank, you will see the bank manager, you will be given a form, you need to look for guarantors, you need to attach some particulars, your contract if you are employed, your payslip number. You need to attach maybe your previous three pay slips. You need to get maybe some ID, photocopy for the guarantors and all that. So it may even take a month for you to access that bank loan. But for the mobile loan apps, I can say that they are instant. So long as you are not listed [with a Credit Reporting Agency], so long as you qualify, then you will just download the app, apply [and] within five minutes maximum when you are on a good network and you meet the required threshold, you will get the money. They are instant and they help a lot during emergencies."*

P11 similarly added that the quick loan disbursement from mobile loan apps is particularly helpful during emergencies: *"It's quite helpful, especially when you have an emergency as compared to other loans like [from] banks. Yeah, because [with] banks, they have so many paperwork and processing time is not quite convenient when you're having an emergency."*

A few participants mentioned using mobile loan apps because of promotions or recommendations, with P14 stating: *"It was the most commonly used app on campus. Plus they had this feature; if you refer [sic] someone and they used your code, [and] they apply for their first loan and pay it [back], they give you 500."* P15 mentioned using loan apps because of the convenience derived from their integration with existing mobile money services such as M-Pesa: *"It's convenient; that linking between the app and mobile payment; because if you can transact easily to M-Pesa and you know M-Pesa is widely used in Kenya; it's an advantage and also convenient."*

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

3.4.2 User Perception of their Credit Score Calculation

As loan apps vaguely mention that they compute users' credit worthiness through data collected from users' smartphones via permissions, we asked participants how they think their credit scores are calculated. Our results indicate that most participants do not know how this is done, with a majority anticipating that their credit score is calculated over time as they borrow and repay. For instance, P11 said *"I'm not really sure but one thing I know [is that] once you pay [back] on time, they will increase your loan limits."* Several participants also speculate that the employment details they provide on sign up are used, with P7 stating: *"They ask for information on how much you earn and also the type of employment; are you a business person? Are you employed? Is the employment permanent or contractual?"*

A few participants anticipate that these applications check their credit score on Kenya's Credit Reference Bureau (CRB) [159] while others believe that the apps check their transaction history from their messages due to the prevalence of mobile money services. For instance, P2 said: *"I think they just check your M-Pesa messages like transactions, because*

among the first permissions you give them is your messages app."

While several participants correctly allude to mobile loan applications generating their credit scores from the data accessed from their smartphones either during registration or via phone permissions [2, 57], a majority of participants are unsure about this process. This suggests an opportunity for mobile loan applications to genuinely and transparently inform users how their credit scores are calculated to increase trust. This could be through updates to their privacy policies to detail how information is collected and used from users' devices or via transparent communication when requesting permissions.

3.4.3 User Understanding of Permissions

As understanding permissions' usage is fundamental in protecting privacy when using mobile apps, we asked participants to explain their understanding of the usage of each permission required by their most frequently used loan app. Note that mobile loan apps indicate that access to these permissions is required to calculate users' credit scores. These results are presented in Table 3.4. While participants generally have an idea of what some permissions are used for, they do not understand the use of a majority of the permissions. Particularly, most of the participants do not know what the telephone, storage and camera permissions are used for by mobile loan apps, confirming prior research on general comprehension of Android permissions in Western contexts [45].

Contacts A majority of participants believe mobile loan apps use their phones' contacts to follow up on their loan if they default, with P13 saying: *"I think it's because, once I default, they can call those people."* As access to contacts allows the app to read all the contacts on a user's smartphone, this indicates that most users correctly understand how this permission can potentially be used. Further, as we discuss under concerns in Section 3.4.4, this has happened to some participants where their contacts are contacted when they default in loan repayment, despite the app not mentioning that this information will be used in this manner.

At the same time, a few participants incorrectly indicated that access to their contacts is required for the app to contact the participants themselves. This is incorrect as the apps contact users through SMS or their phone numbers captured from the registration process or via the telephone permission, rather than through their contacts' permission.

SMS Most participants believe that loan apps use the SMS permission to check financial transactions on their phones (mostly because of the prevalence of mobile money services), send them SMS reminders to pay back loans, or just know their frequently contacted people. As the SMS permission can be used to read, send, or receive messages to or from the user's smartphone, most users once again provide reasons consistent with this. For instance, P20 mentions that access to their SMS helps the mobile loan apps to calculate their credit worthiness, inline with reasons provided by some of the mobile loan apps themselves [2,57]: *"Of course, in your phone, you have M-Pesa messages. They use part of that to gauge how much they can give you and your ability to pay back."* However, P14 incorrectly mentioned that access to their SMS is needed so that the app can send messages to their contacts: *"For messages, I think it's because they usually spam your contacts if you don't pay your loan."* This is incorrect as these applications send messages directly to users' contacts accessed via the contacts permission, rather than through the participants' SMS.

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

Table 3.4: Permissions' Use by Mobile Loan Apps.

Permission	**Permission's Actual Use**	**What Participants Mentioned**
Contacts	Read & edit contact list	Call/SMS users' contacts for defaulting (17) Access or confirm guarantors (3) Call users (2)
SMS	Read, receive, and send SMS	Check transactions (10) Send SMS reminders to pay (5) Know frequently contacted people (4) Check defaults for other loans (2) Phone verification (2) To send messages to users' contacts (1) Send users news updates (1) Promotional texts (1)
Telephone	Access phone no. & network info	Don't know (5) Used to send the users money (3) Reminder calls (3), Track users (2) Confirm phone ownership (2) Check frequently contacted people (1) Check phone type (1), Call users' contacts (1) Promotional calls (1)
Location	Access location	Track users (14) Confirm against user-supplied location (5) Don't know (2), Customize services (1)
Storage	Access files, media, or photos	Don't know (12) For installation or storage of install files (3) Install backdoor (1) Access files (1) Check other apps on the phone (1)
Camera	Take photos & record video	Don't know (7) Take photo or upload documents (6) Assess users' ability to pay from looks (3) Spy on users (1) Track users (1)
Calendar	Read & edit calendar events	Know users' pay date (5) Record keeping (2), Locate users (1) Know borrowing date (1) Don't know (1)
Microphone	Record audio	Talk to an agent via the app (2) Don't know its use (2) Record users (1)

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

Storage While the storage permission can allow an app to access and modify media, photos, and other files on the phone's memory, most participants do not know the use of this permission to mobile loan apps. Only P18 mentioned that this permission allows the app to access files, for example their payslip that might be stored on their phone. A few participants incorrectly mentioned that this permission is required for the app to install on their device. This is wrong as applications do not require access to this permission to be installed. P1 wondered how the loan is related to their phone's storage: *"How is my storage going to help? The money is not going to eat up my storage. That's so funny."*

Camera While most participants do not know what the camera permission is used for by mobile loan apps, several correctly indicated that it is required to capture and upload photos among other documents that might be required as part of the loan application process. Interestingly, most of these participants indicated that the camera can also be used to secretly capture and upload their photos to the loan apps when they are unable to pay back loans, with P20 saying: *"For the camera, I think as long as you have the app installed and probably you don't pay their loan, I think they use the camera to take a picture of you unknowingly, and probably put it out there so that they can shame you."*

Calendar Most participants believe that access to their calendar can help the mobile loan app determine their pay dates, with P1 saying that they *"think the reason is to know when you usually get your money."* While this is technically correct if users have saved their pay dates on their calendar, this access also allows the app to create, edit, and even delete events on the smartphone's calendar which participants did not mention. P12 was apprehensive about the use of their calendar: *"Honestly, I would ask you the same question. Why do they need my calendar? It's not like my calendar is the one that's going to pay for the defaulted loan. So why do they need it? It doesn't make sense."*

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

Overall, while users seem to have a good idea of how some of the permissions are used, they either do not know or have incorrect understanding of how most of the permissions are potentially used. This confirms prior work [45, 79] that has shown that users generally struggle to comprehend Android permissions, despite vast design improvements [1].

3.4.4 User Concerns with Mobile Loan Apps

When asked about concerns they had with mobile loan apps, participants provided diverse responses ranging from high interest rates to privacy concerns. These are discussed below.

Concerns with Loans A majority of participants were concerned about the high interest rates that are charged by mobile loan applications when offering loans, with P1 saying *"their interest [rate] is so high, as much as 20 %."* P9 added that *"comparing them to maybe banks or SACCOs, or any other financial institutions, you find that their interest [rates] tend to be extremely high."* Several participants further complained about growing interest rates

or penalties when they fail to repay the loans on time, with P16 saying *"they do increase their loan if you default to pay within an agreed period of time."* Other concerns relating to loans mentioned by participants include the short repayment period offered, with P8 stating that *"the duration required for payment is usually not that sufficient."* Some participants complained about these applications deducting interest upfront before disbursing the loans to them, while one participant said that the loan amounts offered by these apps are negligible.

These results suggest the need for regulation of mobile loan applications. Unlike traditional financial institutions such as banks which are well regulated in terms of their interest rates and other repayment terms, mobile loans apps are relatively new and lack proper regulations. This unfortunately leads them to exploit vulnerable customers who are unable to secure loans from traditional financial institutions due to a lack of collateral or formal credit history. Fortunately, promising regulations are starting to emerge for example in Kenya [112], to protect users of mobile loan applications.

Concerns (and Lack Thereof) with Permissions After participants had reviewed all the permissions required by their most commonly used mobile loan application, we asked them which permissions were concerning and non-concerning to them. Table 3.5 summarizes the permissions participants were concerned about. Almost all participants were concerned with these apps' access to their contacts, with a majority uncomfortable with these apps contacting and harassing their contacts when they default. For instance, P1 stated: *"They will start calling your parents or they'll start calling your brothers and sisters because they've got your contacts. They've seen whatever the contacts that you have, they just call anyone, even someone that is not into that business of you borrowing or not borrowing. They will tell them that this person has taken money from us, he is stealing from us. So you get [that] they've tainted your name trying to blackmail you so that you can pay back their money, as much as your intentions were not to steal."*

P8 was particularly worried about their contacts getting threatened when they default

Table 3.5: Concerning Permissions of Loan Apps.

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

in repayment, even though most of these contacts are not provided as guarantors for the loan: *"They get in touch with them and threaten them, telling them to ask the loan applicant to pay the amount or they will access that person's phone and deduct that amount from them; and yet, you hadn't listed that person as a guarantor."* P11 narrated how one app contacted their father-in-law when they once defaulted, making them embarrassed: *"They called my father-in-law. Do you know someone called [participant name?] Remind her to pay our loan worth [Ksh.] 6 000. Then they also sent him countless messages. I felt bad and embarrassed. I had to apologize to my father-in-law."*

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

Table 3.6 shows the permissions that participants were unconcerned about. Surprisingly, several participants said they were not concerned with these apps' access to their storage, telephone, and camera permissions as they did not understand what these permissions are used for by the loan app. For instance, P19 said they were unconcerned about storage because

Table 3.6: Non-Concerning Permissions of Loan Apps.

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

they *"don't know the reason for allowing the permission"* while P4 was unconcerned about *"telephone because I have not really understood why they need that."*

Several participants indicated being unconcerned with access to their location as they believe it's a legitimate way for the mobile loan applications to follow up with them if they default in repayment of the loan. For instance, P13 stated: *"I don't think they have collateral; if you fail to pay them and disappear, they will undergo a loss. So I really think that the location [permission] is okay. You can't just take a loan and decide to disappear. I think this is a good technique on how they can follow up on the loan."*

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

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

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

Generally, these results indicate that users have several privacy concerns regarding access to their data via permissions by loan apps. Similar to prior research [11, 12], users seem more concerned about access to their contacts, but less so with their storage. However, they are willing to grant access if they believe the permissions are legitimately required by the app. This suggests a need for loan apps to strictly request permissions that are necessary to their operations. Further, they need to transparently indicate the reason for requiring each of the permissions, perhaps at the time of requesting this access.

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

Other Concerns Apart from security and privacy, more than half of participants were concerned about borrowing addiction or temptation from easy access to loans provided by

mobile loan apps. P19 described how they have to constantly borrow from some other loan apps just to pay off loans from other mobile loan apps: *"You are ever in a debt cycle; you have to borrow from this one app to repay this app before the time expires, and then the cycle continues that way; you borrow from this app, pay the other app, borrow again. The time comes, borrow from this app, pay again. And then the cycle continues that way."*

Lastly, some participants indicated concern with getting listed with Kenya's Credit Records Bureau (CRB) [159] upon defaulting, limiting their ability to procure loans or even get employed in future. For instance, P9 stated: *"When you don't pay back, definitely they register you with CRB. Yeah, so of course when you are registered with CRB, you know, you can't access any other loan anywhere."*

Public outcry about the misuse of CRB's Credit Information Sharing system by mobile loan applications led the Central Bank of Kenya to temporarily suspend mobile credit lenders from listing customers who had defaulted in loan repayment to CRB from April to September, 2020 [55]. To be allowed to report customers that default, mobile loan companies must now meet certain stipulations including detailing their technical staffing as well as credit providers [96]. This has been a promising step in alleviating some of the concerns relating to CRB mentioned by some of our participants.

3.4.5 Privacy vs Loan Tradeoffs

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

the access they have to their information: *"You don't know what they want to do with them [users' data]. But again, they say* ***desperate times call for desperate measures.*** *You need the cash, you don't have an alternative."* P16 was unaware these apps had that much access to their data: *"So I had no idea and I had no otherwise because I was in need of money"* while P2 added that they would not grant any of the permissions if they had a choice: *"If it were up to me, I wouldn't even give them access to anything."*

3.4.6 User Behaviour and Suggestions

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

Some participants indicated a need for loan apps to be regulated when asked to share any additional thoughts. P20 acknowledged the convenience they bring but mentioned a need for regulation of their interest rates and data collection practices: *"Apart from the convenience they bring, if something probably could be done in terms of regulation; on how to go about let's say regulating them in terms of their rates; because they have pretty high interest rates. Then again, something about controlling the amount of data they can access from you."*

P15 suggested the need for data protection regulations in Kenya, similar to Europe, to prevent mobile loan apps from accessing more data than they need:*"I don't know who controls issues of data privacy in Kenya or anywhere else, I probably should think they should have control. Like we have issues of GDPR in Europe. If they have that implementation in*

Kenya, it would be good, because I think they are accessing more than what they need."

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

3.5 Discussion and Conclusion

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

3.5.1 Importance of Loan Apps in the Majority World

Our results highlight the important financial gap that mobile loan applications seem to fill in majority world countries. As many people in these populations remain unbanked often with no formal credit history or collateral, mobile loan applications provide their best chance to access credit that can be used to meet their personal financial needs or fund their enterprises. Therefore, with proper legal frameworks, for example those used to regulate other players in the financial industry such as banks, these applications can improve financial inclusion in these communities while not exploiting their customers, for example through high interest rates or misuse of their data. Such regulations are promising, and are already being discussed and advanced in countries such as Kenya [112].

3.5.2 Concerns with Mobile Loan Apps

Despite benefits in enabling many unbanked people access loans, our interviews reveal strong resentment from users towards these applications from a privacy perspective. This is because these apps collect significant sensitive user data through phone permissions as part of verifying and generating users' credit scores. At the same time, they seem to either misuse or fail to accurately inform users how this data is used, with some participants mentioning that their contacts are called when they default in repayment, despite the apps not mentioning they will use their data this way. This is contrary to what most mobile loan applications postulate, with the founder of Tala, a popular loan app, claiming that users have no privacy concerns with Tala [2]. To this end, mobile loan applications need to transparently inform users how they collect, use, and secure their sensitive data. This can be through improvement of their privacy policies to detail why they collect and how they use different data from their users, instead of vaguely stating that the data is used to calculate users' credit worthiness. Relevant government and industry regulation can play a big role in enforcing this, as similarly recommended by Bowers et al. [19] for mobile money services.

3.5.3 Privacy versus Loan Tradeoffs

While a majority of participants indicated privacy concerns with mobile loan applications, most of them overlook these concerns to procure loans. This is not surprising as prior work [58, 146] suggests that users tend to choose convenience over privacy or security. Nonetheless, consequences from privacy malpractices by some of these applications can be far reaching. For instance, when these applications call users' contacts without informing them, they breach the privacy of the users themselves as well as their contacts' who were not even involved in procuring the loan in the first place. Therefore, application markets should consider removing applications that outright invade users' privacy from their stores. A good starting point would be regularly checking user reviews for these apps on their platforms, and investigating and possibly removing applications that seem to infringe on users' privacy.

3.5.4 (Mis)understanding of Permission Use

Despite design improvements for Android permissions [1], we find that many users still misunderstand or do not know what certain permissions are used for by loan apps, confirming prior work [45, 79] on general comprehension of Android permissions. Particularly, most users do not understand what the telephone and storage permissions are used for. Strikingly, users seem unconcerned with access to these permissions because of being unaware about how they are used. Nonetheless, Android should consider using permission names that are more easily understood by users, as users seem to better understand permissions such as contacts, SMS, and location, perhaps more so than storage and telephone.

3.5.5 User Education

After learning about the sensitive data that mobile loan applications access on their smartphones, several participants indicated they would either avoid these applications all together or would be more careful when using them in future. This suggests that educating users about security and privacy is a promising way to guide them towards better security behaviour. This could be through trainings at institutions as well as using advocates to create more security awareness, as recommended by Haney and Lutters [56].

3.5.6 Over-privilege of Mobile Loan Apps

Prior work [9, 76, 81] has shown that a majority of mobile applications request unnecessary permissions either to gather valuable user data or because of developer errors. Similarly, our study finds that the most common mobile loan applications in Kenya collect significant sensitive user data through phone permissions, with the most common loan apps requiring access to users' contacts, SMS, location ,and storage. While they claim to use this information to calculate users' credit worthiness [2, 57], some of these apps end up misusing this information. While prior work [177, 178] recommends that mobile applications should provide contextual information when requesting run-time permissions to improve trans-

parency, our results suggest that loan app users' motivation to get loans far outweighs their privacy concerns. Therefore, application markets can once again play an important role by investigating and removing invasive apps from their stores to protect the privacy of not just loan app users, but all their users in general. Mobile loan app developers, on the other hand, should follow the least privilege approach recommended by Android [1] and only collect user data that is necessary to their operations.

3.5.7 Recommendations

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

Chapter 4: Security and Privacy Challenges and Advice at Cybercafes in Kenya

This chapter details security and privacy challenges and advice at cybercafes in Kenya. As the Kenyan government moves to digitize most government services, many people have increasingly turned to cybercafes to access essential services as ownership of personal computers remains relatively low in Kenya [25]. However, the use of public computers can introduce a lot of security and privacy challenges and risks for users. To explore these challenges and risks, we conducted $n = 36$ semi-structured interviews at cybercafes in Kenya: $n = 14$ with cybercafe managers and $n = 22$ with cybercafe customers.

Despite the fact that cybercafes serve a crucial role in Kenya e.g., by enabling access to government services, we find that most customers face challenges with computer usage as well as security and usability challenges with account creation and password management. As a workaround, customers often rely on the support and advice of cafe managers who mostly direct them to use passwords that are memorable, e.g., simply using their ID numbers or names, leaving them vulnerable to password guessing attacks. These results suggest the need for more awareness about phone-based password managers, as well as a need for computer training and security awareness among these users. There is also a need to explore security advice beyond Western peripheries to support the safety of broader populations.

This chapter is based on work originally published at the 44th IEEE Symposium on Security and Privacy [103]. I have permission from my coauthors and publishers to use this work in my dissertation. Copies of all copyright permissions are in Appendix D.2.

- Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In Proceedings of the 44th IEEE Symposium on Security and Privacy, Pages 570-587, San Francisco, CA, USA. May 2023 [103]. **Distinguished Paper Award.**

I came up with the idea for this project, designed the interview protocol, performed initial pilots, collected the data, analyzed it, and wrote the paper. Miles Grant assisted with secondary qualitative coding, while Karen Sowon and Animesh Srivastava provided feedback on the interview protocol design. My co-authors provided a lot of feedback throughout the research process, from ideation all the way to writing the manuscript.

4.1 Introduction

Cybercafes are privately-operated facilities with computers, printers, and other equipment where customers pay to access the Internet and perform other computer-related tasks [154]. Quite popular in the early days of the Internet when broadband internet access was less common, cybercafes have recently fallen out of favor in Western countries as personal computers with Internet access in the home become ubiquitous. In majority world countries, however, cybercafes remain an extremely common way for many users to access the Internet and other digital services as ownership of personal computers remains relatively low [10].

In Kenya, the government recently transitioned to an e-government portal called eCitizen [39] to improve service delivery. This portal provides a one-stop electronic access to common government services including immigration, drivers' license application, and renewal, among others. However, only around 8.8% of the 12 million Kenyan households own a computer or laptop [25]. Most Kenyans have thus turned to cybercafes to access these services. Many of these users may have never used a computer and likely face significant challenges, including computer usage, account creation, and password management.

In this study, we explore the most common services accessed at cybercafes in Kenya as well as the challenges, particularly related to security and privacy, that customers encounter at these facilities. We are also interested in exploring the security and privacy advice and support offered by cybercafe managers to their customers. More specifically, we seek to answer the following five research questions:

RQ1: What are common services that are sought or provided at cybercafes in Kenya?

RQ2: What security and privacy challenges do customers encounter at cybercafes?

RQ3: What security and privacy advice and support is provided at cybercafes and how does it impact cybercafe customers' digital security and privacy?

RQ4: What advice do users in Kenya consider important for staying safe online?

RQ5: What are general security and privacy concerns and practices at cybercafes in Kenya?

To answer these research questions, we conducted $n = 36$ semi-structured interviews at cybercafes in Kenya: $n = 14$ with cybercafe managers and $n = 22$ with cybercafe customers. To recruit participants, one researcher, who is a native Kenyan, visited 14 cybercafes in Nairobi, Kenya in July 2022. The researcher made efforts to visit diverse cybercafes located in Nairobi's Central Business District and in residential areas. As most cafe managers and customers were busy, only five non-recorded interviews with managers were conducted on-site. For the other participants, the researcher collected their contacts and conducted the interviews remotely through direct phone or WhatsApp calls at times that were convenient to the participants. These interviews were all conducted between July and September, 2022 and were audio-recorded and transcribed with permission from the participants.

We asked cybercafe managers to detail the equipment at their facilities, including the number of computers and OS update practices, followed by services that customers most commonly use along with any challenges they encounter. We then asked the managers about the advice and support they offer to their customers and any standard practices they have at the cybercafe to protect customers' security and privacy. Lastly, we asked managers about their top three advice for staying safe online, similar to prior work [23, 71]. For customers, we asked about the services they use at the cybercafe, as well as any challenges they faced. Afterward, we also asked them to share any security and privacy advice they have received at cybercafes, followed by advice they consider important for staying safe online.

Our results indicate that cybercafes continue to play a critical role in the majority world by allowing many people to access printing, government, and other internet services. In

Kenya, most customers use cybercafes because they do not have access to personal computers or printers, and rely on the assistance from cafe managers to complete computer-related tasks. Yet, customers experience significant usability and security challenges around general computer usage, online account creation, access, and recovery. Password management is particularly challenging for many customers who experience difficulty selecting and recalling passwords across accounts, leading to many getting locked out of their accounts.

Most customers rely on advice and support from the cybercafe managers when navigating these challenges. Many customers are novice computer users, at best, and tend to regularly forget their passwords and sometimes even emails used to register their accounts. The managers end up selecting passwords for them that are easy for the customer (and the manager) to remember, such as customers' national ID numbers, names, children's names or some combination of these. Some managers directly manage the account passwords for some of their customers, with one manager using the same password for all their customers. Unlike security and privacy advice in Western contexts [23, 71], we additionally find that the most important security and privacy advice in Kenya centers around the use of public or shared computers, with most managers and customers indicating that logging out of their accounts after using these facilities is their top advice for staying safe online.

As a community, we need to consider the security and privacy needs of broader user classes, rather than designing all solutions for Western contexts. For example, while several managers and customers do not saving passwords in the browser of public computers to protect themselves, it is still critical to explore alternative ways of password management that better fit these users' needs. Current password managers, either browser-based or third-party, are not good fits but mobile phone-based password management offers some promise as phone usage is high. At the same time, device-sharing is common, complicating such solutions. We explore these challenges, offer recommendations, and suggest promising areas for future work, including general computer training and security awareness as well as the need for research on security and privacy advice beyond Western contexts.

(a) Customers Using Computers in a Cybercafe.

(b) A Customer Receiving Assistance in a Cafe.

Figure 4.1: Customers at Different Cybercafes Located in Nairobi, Kenya, in July 2022.

4.2 Background on Cybercafes in Kenya

A cybercafe, also known as an internet cafe, is a facility typically equipped with computers, printers, and other equipment where customers pay to access the Internet, play online games, edit, scan, photocopy, and print documents among other computer-related tasks [154]. The first cybercafe, known at the time as cyberia, is believed to have been established in London in the United Kingdom in 1994 [68]. It became an instant success as the Internet was still in its early days and most people did not own personal computers or laptops. More cybercafes were subsequently established in other places and countries around the world. However, recent ubiquity of the Internet coupled with the proliferation of personal computers have led to a rapid decline of cybercafes, particularly in Western countries.

While smartphone adoption and usage has been growing in majority world countries [4], many people in majority world countries still do not own personal computers or laptops, with only an estimated 7.7% of households in Africa owning a computer in 2019 [10]. Coupled with growing social media adoption as well as digitization of government services, many users in this region are increasingly relying on cybercafes to access essential services.

Kenya is one of the countries in Africa that have recently transitioned to an e-government portal to "hasten service delivery, reduce transaction costs and safeguard revenue" [3]. Known as eCitizen [39], the portal provides access to essential government services including immigration, land transactions, business registration, and motor vehicle purchase, and registration. To use eCitizen, users create an online account on the portal, fill out the relevant forms, make the required payments and print the filled forms before finally presenting them to the relevant government department. This portal stores a significant proportion of sensitive user information, including their identification and passport details, date of birth, address, and their personal details. It is therefore imperative to protect these accounts.

However, with only about 8.8% of 12 million Kenyan households owning a computer, laptop or tablet [25], a large proportion of Kenyans have turned to cybercafes to access these essential government services (examples of cybercafes in Nairobi, Kenya, are found in Figure 4.1). Even those that own computers often do not have printers at home and usually visit cybercafes whenever they have to print, scan, or photocopy documents outside of work or school. Further, some cybercafe customers are novice users and have never previously used a computer nor created an online account, and face significant challenges throughout.

It is the goal of this research to understand the challenges encountered by cybercafe users, particularly those related to security and privacy or account management, and the advice and support that these users receive at the cybercafe from other customers and the cybercafe management. We also seek to understand the impact of this advice on the customers' security and privacy perceptions and practices at the cybercafe and beyond.

4.3 Methodology

We conducted $n = 36$ semi-structured interviews with Kenyan cybercafe customers and managers to explore security and privacy challenges and practices at cybercafes: $n = 14$ interviews with cybercafe managers (M01-14) and $n = 22$ interviews with cybercafe customers (C01-22). We also investigated the scope and nature of advice that is provided

to customers at these facilities and its impact on their security and privacy actions and perceptions. In this section, we describe our recruitment procedure and interview script followed by our approach to data analysis. Finally, we discuss limitations and ethics.

4.3.1 Recruitment and Demographics

To recruit participants, one researcher, who is a native Kenyan, visited 14 cybercafes in Nairobi, Kenya in July 2022. Additional participants were recruited through snowballing [52] where participants recommended other potential participants that have previously or currently use, work, or own cybercafes in and around Nairobi. We made all efforts to diversify our sample, with the researcher visiting cybercafes located both in Nairobi's Central Business District as well as in residential areas. We had a total of $n = 36$ participants, $n = 14$ cybercafe managers and $n = 22$ cybercafe customers.

Participants had to be at least 18 years old and previously have or currently use, own, or work at a cybercafe in Kenya. Most of the cybercafe managers own the cybercafes (10 were owners while 4 were employed there) and had between one to five years of experience owning or working at the cafe. While most of the managers were men aged between 26 to 30 years, we had an even split between men and women participants for the customers. Most customers were young and between 18 to 25 years. Tables 4.1 and 4.2 summarize the cybercafe managers' and customers' demographics.

4.3.2 Interview Procedure

The interview procedure centered around the research questions outlined in Section 5.1. The protocol was also informed by prior studies that explored security and privacy where users share computing facilities, such as libraries in the US [37, 91], and research on users that rely on others for digital assistance, for example newly resettled refugees in the US [145]. Similar to studies that have investigated security and privacy advice [23, 71], we also explored the security and privacy advice that participants in Kenya consider important for staying safe

Table 4.1: Demographics of Cybercafe Managers.

		No.	%
Gender	Women	3	21.4
	Men	11	78.6
Age	18 - 25	2	14.3
	26 - 30	5	35.7
	31 - 35	4	28.6
	36 - 45	1	7.1
Own Cybercafe	Yes	10	71.4
	No	4	28.6
Cybercafe Experience	Less than a year	3	21.4
	1 - 5 years	9	64.2
	Over 5 years	2	14.3
Education	College	6	42.9
	Bachelors	7	50.0
	Masters	1	7.1

Bachelors and Masters degrees in Kenya are offered by universities, with colleges mainly offering vocational training.

online and how this compares to Western perspectives. The full interview procedure is available in Appendices B.1.1 and B.1.2.

Cybercafe managers were interviewed first as a way to broadly explore general practices at cybercafes. We began by asking managers general questions about their experience level with cybercafes, the number and type of equipment in their facilities, and how often these devices are updated. We then inquired about common services that users typically seek, along with any challenges they face. Following, we asked them to detail any assistance and advice they offer to their customers, both generally as well as relating to security and privacy, if they did not mention it themselves. We then asked for their top three security and privacy advice for staying safe online and if they had any standard practices at their cybercafes to protect customers' security and privacy.

For the cybercafe customers, we first asked them to state their reasons for using cybercafes and what they like and dislike about using cybercafes. We inquired about how

Table 4.2: Demographics of Cybercafe Customers.

		No.	%
Gender	Women	11	50.0
	Men	11	50.0
Age	18 - 25	15	68.2
	26 - 30	6	27.3
	31 - 35	1	4.5
Own a Computer	Yes	16	72.7
	No	6	27.3
Employment	Employed	7	31.8
	Not employed	14	63.6
	Prefer not to say	1	4.5
Education	High school	7	31.8
	College	4	18.2
	Bachelors	9	40.9
	Masters	1	4.5
	Prefer not to say	1	4.5

frequently they visit cybercafes, along with factors they consider when selecting a cybercafe. Following, we asked them to describe any challenges they have faced when using cybercafes and any assistance they received, both generally and specifically relating to security and privacy. Similar to the managers, we also asked for their top three advice for staying safe online. Lastly, we asked customers questions about their mobile phone usage, including the websites they access, whether they share their devices with others, and any authentication they use to protect access to their devices.

4.3.3 Data Collection

The study was piloted twice. Foremost, two cybercafe managers in Kenya participated in two separate preliminary interviews conducted through WhatsApp calls. After an iteration based on their feedback, two mock interviews were conducted with qualitative researchers, with each acting as a cybercafe manager and customer. Based on that feedback, we added more branching questions and deeper probes to the interview questions [28].

One researcher, a Kenyan native, visited 14 cybercafes for recruitment and data collection in Nairobi, Kenya in July 2022. Nearly all cybercafes were small, containing between 1-to-10 computers (one had 20 computers) that were all running Windows. Two cybercafes also had CyberCafePro [33] to help manage user sessions and payment. A majority of the cybercafes had one or two printers, with only three cybercafes having more than two.

Five non-recorded interviews with managers were conducted on-site. However, since most of the managers and customers were busy using the cybercafe services or assisting customers, the researcher collected their contacts and conducted recorded interviews later at their convenience through WhatsApp or phone calls. These interviews were conducted between July and September 2022. Each participant was compensated with 2 GB of internet data or 125 minutes of call time for participating. On average, the cybercafe manager interviews lasted 41 minutes while the customer interviews lasted 30 minutes.

All interviews were audio-recorded except five on-site interviews with cafe managers who were uncomfortable being recorded at the cybercafes; the interviewer took notes. While all interviews were conducted in English, one of Kenya's official languages [113], participants occasionally provided responses in Swahili. These were translated to English during transcription by the Kenyan researcher who is fluent in both languages.

4.3.4 Data Analysis

We qualitatively analyzed the interview transcripts and notes using open-coding techniques [132]. One researcher independently coded all the interview transcripts from cybercafe managers and customers to develop a primary codebook. A secondary coder then used this codebook to independently code half of the interviews from the cybercafe managers and half of the cybercafe customer interviews. Throughout the process, the two researchers frequently met to resolve coding differences and update the codebook. The researchers also used these meetings to discuss broader themes emerging from the study [99]. The results in Section 5.3 are based on the primary codebook available in Appendix B.2. Due to the

qualitative nature of this work, we do not report counts to avoid implying generalizability. Instead, we use quantifiers such as most and few to show the prevalence of common themes.

4.3.5 Limitations

Our study has several limitations. Foremost, our sample size is relatively small, urban, and limited to participants that agreed to participate. A few potential participants, particularly managers, declined to take part for various reasons, including being busy or concerns about leaking competitive information. While we do not claim our results to be fully representative — there are likely themes that we could not capture due to the size or recruitment of the sample — we argue that the themes we did identify are likely common and relevant at cybercafes in Kenya, and potentially other regions with similar demographics.

This study may also suffer from social desirability bias where participants try to look more favorable to an outside observer, particularly if that behavior may cast them in a poor light. We tried to mitigate this by encouraging participants to be honest throughout, citing that we were not testing their knowledge but simply interested in their honest thoughts and real practices. Our results suggest participants were forthcoming, with some participants going as far to share what may be considered unflattering behavior. A few managers, for instance, admitted they do not "interrupt" customers when they are facing challenges so that they can spend more time and ultimately more money at the cybercafe.

Lastly, the top security and privacy advice reported by cafe managers and customers could be attributed to these users' reliance on public computers. Despite cafes' popularity, more work is needed to explore security and privacy advice in Kenya beyond cybercafes.

4.3.6 Ethical Considerations

This study was approved by both our Institutional Review Board (IRB) and the National Commission for Science, Technology, and Innovation (NACOSTI) [109], the body that oversees and approves research activities in Kenya. We fully informed participants about

the purpose of the study, its duration, and any anticipated risks. Participants were also free to withdraw from the study or not respond to any uncomfortable questions without any consequences. Additionally, we did not collect any personally identifying information (PII) from participants to minimize any risks of potential disclosure. Any PII captured was scrubbed off the transcripts before we performed qualitative analysis.

4.4 Results

This section is structured around our five research questions. We first discuss the important role that cybercafes play in enabling people to access government and printing services in Kenya, followed by challenges that customers encounter at these facilities. Afterward, we detail the advice and support provided, followed by security and privacy concerns, practices, and behaviors at the cybercafes and beyond. Since our results are qualitative in nature, we do not report counts to avoid implying generalizability. The counts provided in Table 4.3 are only meant to highlight common themes and unique perspectives.

4.4.1 Role of Cybercafes in Kenya

Reasons for establishing cybercafes When asked their reasons for establishing the cybercafe, most managers indicated doing so to address the demand for Internet and printing services, particularly relating to government services, as well as to provide for their livelihoods. M03 stated that they established their cybercafe because people need *"the cyber services, things like printing and other Internet services."* M14 *"saw it as one way of helping the society and then on the other hand, at least generating some small income."* Those employed at the cybercafes as managers, who were not owners, indicated that they are interested in and passionate about computers, or that they have the relevant skills to operate them from school or past experiences.

Common services provided at cybercafes Printing and government services accessed via eCitizen [39] are by far the most widely-used services at cybercafes. M10 indicated that *"there are these online services, you know them, application for police clearance, you have application for NTSA*[1] *services . . . application for smart DL, you can have PSV*[2] *badge, you can also have passport application, that is the department of immigration. So most of my customers . . . maybe deal with government services."* Other common tasks performed at the cybercafe include job applications, email access, photocopy, assignments or school projects, document typing or editing, scholarship or school applications, social media access, remote work, movie streaming or downloading, gambling, filing of taxes through iTax [13], and computer training. Beyond cybercafe services, some cybercafe managers further indicated that they sell phones, computers, stationery, and other equipment that customers often require. Other services mentioned by more than one cybercafe manager included gaming, banking, and mobile money services as well as repairs. For repairs, M14 stated that *"you will find that I also have a category of customers who bring machines to be repaired, who bring machines to be installed for the operating system."*

Services requested but not provided When managers were asked about the services their customers sought, some wanted services that were not provided or are illegal. This included certificate or document forgery, website design or development, music downloading, phone formatting, photography, bulk, and passport photo printing. Most managers are hesitant to forge documents or download music for their customers due to personal integrity or legal liability. As an example, M06 stated that *"forgery is not healthy, it's like you're lying to somebody that this person is so able to have this thing, like somebody never did form four*[3] *but you're giving this person a form four certificate."* M03 wondered *"what happens if you're caught doing it"* while M09 said they do not download music for their customers

[1]The National Transport and Safety Authority (NTSA) is the governmental body in Kenya that manages the road transport sub-sector.

[2]A public Service Vehicle (PSV) license is a document issued by NTSA to drivers who serve the public sector by offering transport services.

[3]The final year of secondary school in Kenya is known as form four.

as they do not have a license[4] to do so: *"I don't put Kenyan music or East African music for customers because that is illegal in Kenya, because unless you have the copyrights from the government, you cannot put those kinds of songs. When they find you, you are arrested."* M08 even mentioned that *"some people want to disable their partners' Facebook accounts."* For the advanced tasks including website design and bulk printing, the managers often indicated that they lack either the required expertise, equipment or time to offer them.

Factors when choosing a cybercafe to visit When choosing a cybercafe, most customers consider the environment where the cafe is located, the manager friendliness or their ability to offer assistance, the Internet speed at the cafe, and cost. For instance, C08 stated that one of the things they consider *"is the person behind the counter. How are they receptive? How are they addressing my issues?"* Other factors that customers often consider include proximity of the cybercafes to where they are or live, the state or speed of the cybercafe computers, availability of working space, electricity stability, physical safety, and privacy. Regarding privacy, C02 stated: *"I don't like those [cybercafes] that are open . . . you have a computer here and then there's no partition. It's just like somewhere where you can find some privacy and do your work without somebody peeping at what you're doing."*

Additional cybercafe positives Beyond the relatively fast Internet available at cybercafes, most customers appreciate the availability of equipment, such as computers and printers, that they may not have access to regularly. C01 indicated that *"in the cybercafes, I easily get the printers and maybe more advanced equipment that I may want to use in my projects."* Several customers also mentioned affordability of services, availability of assistance and perhaps surprisingly, privacy as other things they appreciate about cybercafes. C19 mentioned that the cybercafe they use is *"partitioned in such a way that the neighbor, the person sitting next to you can't see or access what you're doing."* C03 even mentioned that they feel they have

[4]If you play music in your business, or want to use music in the promotion of a product, you need clearance from the owners of that music.

more privacy at the cybercafe compared to working from home: *"There's a lot of privacy there, more than using my own laptop, and my son also sometimes would like to use it [at home]. So in the cybercafe, I think there is some privacy there."*

Summary Cybercafes play an important role in Kenya by providing customers access to printing, government, and other Internet services that they may otherwise not have access to due to a lack of required equipment such as printers or personal computers. Customers additionally seem to prefer cybercafes where the managers are friendly and can therefore assist them whenever they encounter challenges.

4.4.2 Challenges at Cybercafes

Cybercafe challenges When asked for general challenges or drawbacks when using or operating cybercafes, an overwhelming majority of cybercafe managers and customers mentioned slow internet that sometimes makes it difficult to access websites or perform other Internet-related tasks. C13 said that the *"challenge I have faced is the network. Sometimes it's slow, because we have so many people in that cafe, using the Internet."* M13 underscored the importance of having an alternative internet plan in case of connectivity issues: *"Even if I'm using a good internet connection from fiber, sometimes there is a downtime and you don't understand why. So . . . you must always have a backup plan."*

Other common challenges include electricity outages, old or faulty equipment, and slow computers. Several customers also complained about the printing quality in some cafes, with C02 saying that *"there are some cybercafes where the printers are, I think outdated, because once you print, the documents don't come out clearly."* Some customers additionally indicated unhelpful or unfriendly managers, and crowded as well as noisy cybercafes as aspects they disliked about some cybercafes. Some managers cited harassment from the government or law enforcement as well as expensive equipment as additional challenges they encounter. M10 complained that *"with [the] county police, they require a license for*

single business permit, they require license for fire[5]*; they require license for advertisement. But you see, you cannot have all of them. So for my case, I have a license for single business permit. I have an advertisement board, but I don't have the license. I also use electricity but I don't have the license for fire. So the main challenge is that when you hear that county police are around, you have to close your business whether you like it or not, because you will be arrested."* M03 added that *"even though we have paid their licenses, they usually come and rough up the operators inside the cyber."*

Customer challenges The most common challenge that customers face at cybercafes is generally not knowing how to use or operate the computers. M10 said that some customers are sent to the cybercafe, for example by their family members, but forget or do not know what to do: *"Most of the time, you get a person, they don't know how to use a computer, and they tell you I want to do this thing. He has no clue. So you have to start from scratch, and ask him what he has been sent to do."* C08 added that *"when doing things to deal with government tax, filing my returns, sometimes, I don't know how to go about it."* Customers also struggle with either printing, binding or scanning, using certain programs as well as typing. M05 said that *"maybe a customer doesn't know how to type, and the documents he wants to send; he or she is unable to compose the email."*

Another challenge that customers often encounter is difficulty accessing or recovering access to their online accounts because they have forgotten their account passwords. M07 said that *"the main challenges are that sometimes the accounts are not functional, that they have been locked out because of lost passwords."* Several managers also mentioned that some customers usually forget the emails or phone numbers used to create their accounts. M10 said that *"someone comes and tells you: I have a KRA*[6] *PIN, I don't know the email that I used or the phone number that I used [to create the account]. So I find it as a challenge because if someone does not know the email that they used, or the phone number used,*

[5] A fire license in Kenya certifies compliance with fire safety standards.

[6] Kenya Revenue Authority (KRA) is the governmental body in Kenya responsible for the assessment, collection, and accounting of all revenue.

so it means that they have a challenge creating an email, setting up their account." C20 indicated that *"I had forgotten my email, my password . . . and they [cafe managers] helped me."* Some customers, however, give up on the account recovery process as mentioned by M07: *"Maybe you lost your password and this is something that is so common here and now you have a process that you have to follow so that the provider can reset the password. But some of them, they don't want to wait or they don't want to contact the customer care. So they will just leave it and say they don't want to use that site for now."*

Some managers and customers mentioned downtime and bad user interfaces, especially on government websites, as other challenges in accessing user accounts. C04 complained about *"the government systems. When you're browsing, they may be a bit frustrating, maybe system failures in terms of those websites . . . like, our taxing system."* M08 was similarly frustrated about the *"bad user interface from some government sites for example NTSA."*

Customers also encounter challenges when setting up their accounts, with some customers struggling to comply with certain password requirements, not knowing the appropriate password to use, or not caring about passwords all together. This leads to poor memorability of these passwords the next time they need to access these accounts. M10 said that *"most of the people, they are not aware which password they can use,"* while M08 added that *"some sites have specific password requirements, some require a mixture of characters which can be challenging for customers."*

Other challenges that customers encounter include struggling to understand websites in foreign languages and a fear of computers. M08 stated that *"some websites are in foreign languages and customers are not aware about [Google] Translate"* while M01 added that *"some customers fear using the computer."* To navigate these challenges, managers usually provide guidance and assistance to their customers. This is discussed in Section 4.4.3.

Reasons for not facing challenges Customers who have not faced any challenges at the cybercafe indicated that they mostly visit cybercafes that they are familiar with to do familiar

tasks, or that they are experienced with computers. C19 stated that *"personally, when I go to the cyber* [7]*, I know what I'm going to do and I have these specific sites or websites that I'm going to access, . . . and I've been dealing with these, these websites for some time. So I don't get those challenges, unless it's a new site."* C06 cited their computer knowledge: *"You will find that, maybe, more so I have more of the computer knowledge because the work that I always do, it's computer-dependent. So I think it's also my computer knowledge that always makes me not to ask a lot of questions because it is what I use in my day to day basis."* Some customers further indicated that the tasks they do at the cybercafe are easy while others pointed to the availability of assistance as reasons for not experiencing challenges.

Summary There are several challenges at cybercafes, especially relating to internet and electricity outages that often times make their services unavailable. Customers experience challenges with the general usage of computers and other cybercafe equipment including printers, as well as difficulty accessing or recovering access to their accounts. To resolve these challenges, customers often turn to the cybercafe managers for assistance.

4.4.3 Advice and Support at Cybercafes

Account and password management As general computer usage and account recovery are the most common challenges at cybercafes, the most common advice and support offered to cybercafe customers relates to account and password management. Most managers encourage customers to select easy to remember passwords including their national ID card numbers[8], birthdays, phone numbers or some combination. M03 said that *"if we find, like a novice user, in most cases we just use a password that has a feature in them or what they have. So for example, a user has come to just apply for or create an account for government services. In most cases, we use their identity card numbers as their password, or their mobile [phone] numbers . . . A combination of mobile, and year of birth, those common*

[7] Cybercafes are commonly referred to as cybers in Kenya.

[8] An Identity Card (ID) is an identification document with a sequential 8-digit national ID number issued to Kenyans that are at least 18 years.

characteristics that define a person. So we usually give them or create for them just a password they can easily remember."

M05 said that if the customer name is *"John, I use the first letter of your name, your ID [number] and then add a full stop, just to make them remember."* M06 uses a mix of the name of the customers' children and their birthday: *"For the majority of them, I like asking them: What is the name of your first child? When was he born, or she born? Then, let's say it's William. I take, I just use William@2004#."* M04 encourages their customers to only use their ID numbers as words can make these passwords hard to remember due to multiple cases: *"I usually recommend them to use the ID number as the password because with the names of their first-borns, they can forget if the name was in capital or lowercase."*

To help customers recall their passwords, some managers encourage customers to save their passwords in the cybercafe browsers, write the passwords down for the customers, or even select the passwords for the customer. M10 stated that *"in most of the cases, I can say* ***in eighty percent of the cases, I select the password for them;*** *twenty percent, they select the password for themselves."* M06 said that they store the passwords for the customers by writing them down and then providing them when they request: *"They come to you and tell you: What was my password? Then you get where you wrote the password and give the person the password."* M01 uses a standard password for all novice customers so that they can easily provide it to them on request: *"I use a flat password for anyone new to computers; it's the same password for all of them."* C14 said that their cybercafe manager encourages them to save their passwords in the cybercafe browser for seamless access whenever they visit the cybercafe: *"The advice I got was that they are able to save my password so that the next time I visit, I just go through without even asking."*

At the same time, some managers encourage their customers to use passwords that are uncommon or difficult to guess and to not save them in the browsers on the cybercafe computers. M08 tells their customers not to *"use passwords that are common for example phone numbers, ID numbers"* as well as *"common passwords like Godspeed, Godsent."*

M02 asks customers *"not to save passwords in the browser"* while C04 said that *"when you access those cybers, you're told not to save your password for the purpose of privacy."*

Support with tasks Due to challenges using computers, several managers often have to do the actual tasks for their customers. M11 said that *"most customers ask me to do the actual tasks for them as they do not know how to do them or are unable to do."* M02 added that *"some tasks are also more technical for example explaining how to do something in Microsoft Word or Excel can be very hard, so I just have to do it myself."* C10 said that *"most of the time, they do it for you. Printing, photocopy, like they do for you everything."*

Account recovery Since customers tend to forget their passwords, cybercafe managers use various ways to try and recover access to these accounts, including resetting passwords or contacting relevant customer care. M04 said that most customers that forget their passwords *"are old-aged people. They usually come and they have forgotten their passwords. Or you can get the other person has forgotten their Gmail account . . . So I usually use their phone number to retrieve the Gmail account or the password. So when they come, I usually use the verification code through the phone number to retrieve their Gmail [account]."* M08 reaches out to customer support, particularly for local government-related accounts: *"For account recovery, if local, such as the government, I try to make calls to [the] relevant people. If I cannot get assistance, I ask them to go to the help desk of the relevant government service."*

Account recovery, however, is not always successful as some customers usually forget the emails associated with the accounts, or no longer have the phone number used to register the account. M01 said that *"the challenge that's usually hard to resolve is resetting passwords for users who have lost their phone numbers, some people even forget their email addresses. Others have many emails but cannot even remember these emails."* M10 indicated that some customers forget the usernames that are set for their accounts: *"You've created an account for someone, you've created a password, someone comes back and asks you: What username had we used? What password had we used? So it gives you*

a challenge remembering your customers' passwords, the username you had used." To navigate these challenges, some managers write down account details for their customers, encourage customers to save their passwords in the cybercafe computers' browsers, or even select a standard password for all novice customers as described earlier.

Teaching or training customers When customers encounter challenges, cafe managers guide them or teach them how to do the tasks. M09 first *"inquire[s] where they need help. After they have told me this is where I need help, I personally teach him or her. This is where you go, this is what you do so that [the] next time when he or she comes, she doesn't have the problem anymore."* M05 added that they *"advise them to familiarize themselves with computers and some of them come back as our students for computer packages."*

Other guidance and advice To protect their customers' accounts, some managers additionally encourage their customers to always log out and never to save their passwords in the cybercafe computers' browsers. M09 said that *"a lot of customers don't know how to log out of their Gmail accounts . . . So anytime a customer comes to my cybercafe, I must tell them, after you have logged in to your account, please log out and delete the account because I don't want to get in trouble because of identity theft . . . So by the time I'm closing up, I have to check in every computer, which account is not my mine or associated with the cybercafe, and I delete it."* M01 encourages customers using their own computers to constantly update their operating system, while C01 said they were advised not to save any documents on the desktop of the cybercafe computers by a manager.

Sources of advice When asked for their sources of security and privacy advice, a majority of customers and managers often mentioned the Internet, with C03 saying *"I just Google."* Most managers leverage their personal experiences with computers when assisting or guiding their customers. M03 said that *"after doing something for long, you are very much conversant, you get experience on it."* M14 added that *"the advice that I usually rely on by*

the way is based on my personal experience. Because I have dealt with computers, I've been in the IT industry for a very long time. So at the end of the day, there are some things that don't actually force me to go and seek suggestions from people." Managers also reach out to other cybercafe managers when customers experience challenges they are not familiar with. Other sources of security and privacy advice for both customers and managers include school or training, as well as family and friends.

Reasons for (or against) following advice A majority of cybercafe customers follow the advice provided to them by managers because it helps resolve their challenges, they believe the advice helps protect their personal information, or because they trust the cybercafe manager. C08 indicated that *"if I asked them something that I don't know, then I have to take the advice and try it out, but almost all the time it has worked out."* M14 further added that *"most of them have come back to me actually confessing that they did get help, and they're doing well."* C15 follows the advice *"because they are very important in . . . securing the data that I interact with."* M01 pointed to the trust they have developed with their customers: *"Yes they follow the advice, others take time to write it down. They follow the advice because of the trust we have developed. Some will even call me at night to ask for their password, and some even travel from afar just to come and find me."* Some customers also follow the advice from managers because they view or find the manager to be an expert or friendly, or have limited time to perform the tasks which are sometimes very urgent.

At the same time, a few customers sometimes fail to follow advice provided by the managers. Often, the managers said the customers have contradictory beliefs, they are too elderly or have been advised differently. Other times, the customers are skeptical of the advice, do not have time or the tasks they are performing are non-urgent. M08 said that *"some refuse to follow the advice because they may have been advised differently. For example, some believe [that] having many emails is criminal. Some have religious beliefs and believe social media accounts are evil. For example, one came and applied for a job, and I helped*

them create a LinkedIn account. The next day, they came back to ask me to delete it since they were informed it is evil." M08 said that *"some listen with suspicion. Some suspect that I am advising them so that they spend more money here."*

Satisfaction (or lack thereof) with advice For customers that had received advice or assistance at cybercafes, about half of them were satisfied while the other half were unsatisfied with the assistance they had received. Those satisfied indicated that their challenges had been resolved while those unsatisfied often pointed to the manager taking longer than expected to assist them which often forced them to spend more money at the cybercafe. Some customers were further unsatisfied because their challenges were not fully resolved.

Summary Cybercafe managers offer usability and security advice and guidance to their customers, particularly relating to account and password management as well as account recovery. As customers tend to forget their passwords, most managers encourage them to use passwords that are easy to remember, for example their ID numbers. Some managers even select and manage passwords for their customers. Most customers follow the advice provided as they trust the cybercafe managers and view them as experts.

4.4.4 Top Three Security and Privacy Advice

Important advice for staying safe When asked for their top three recommendations for staying safe online, both cybercafe managers and customers mostly provided similar responses, with logging out of accounts after using public computers mentioned the most (see Table 4.3). C20 said that *"when you're using, maybe you want to log into your account and maybe you're not using your phone or your own computer. The best thing is to log out, make sure you have cleared everything that you were doing; maybe on someone else's phone or computer."* The next most common recommendation for staying safe online is avoiding clicking on suspicious links or visiting websites you are unsure of. M13 said they *"avoid clicking websites that are suspicious. Because nowadays, we have so many popups on*

the websites, people tend to click because those pop ups are offering, like, some ridiculous offers about how you can earn this money. . . " Participants further mentioned the use of strong or secure passwords as important. M11 pointed to the use of *"passwords that are not phone numbers or ID numbers, use mixed characters including numbers and words"* while C02 mentioned avoiding *"commonly-used passwords."*

Other important recommendations for staying safe online mentioned by several participants include not saving passwords in the browser when using public computers, using a password for accounts, and not sharing passwords. Participants further mentioned not using public Wi-Fi and using firewalls. While some of the advice mentioned by participants including using strong passwords, multi-factor authentication, and use of anti-virus software match inquiries from Western contexts [23, 71], we find that most of the recommendations center around shared computers at cybercafes, which are relevant to this demographic. This includes logging out of accounts, not saving passwords on public computers, clearing history, and deleting downloads after using the public computers at cybercafes.

Following advice When asked if they follow their top three advice, most customers and managers were affirmative. M07 said that they *"follow them because I work online and I would really hate to be a victim of something that I was aware was harmful. So I do follow them myself and I'm encouraging others to follow them."* Those that do not follow their advice cited the negative usability impact of following the advice or unavailability of options to do so. C14 said that they *"normally use a difficult password and forget"* while M08 said that they *"try to have many levels of authentication but some sites do not have that."*

Not following advice When asked what would happen if they did not follow their top three advice, most participants indicated that they would be susceptible to attacks including viruses, hacking, malware, ransomware, and impersonation. M13 detailed how they once *"clicked on the wrong link and my computer got infected with a very bad virus. So I guess I have also made mistakes before, but it has taught me more to avoid such things."* Several managers

and customers also mentioned unauthorized access, data leaks, loss or manipulation, and financial loss or fraud as consequences of not following their top advice.

Summary Cybercafe managers and customers believe that logging out of their accounts when using public computers, avoiding unknown links, strong passwords, and not saving or sharing passwords are the most important pieces of advice for staying safe online. This advice is slightly different from what other studies in Western contexts [23, 71] have noted. This is possibly a result of users mostly accessing the Internet through shared computers in this region, unlike in Western contexts, where most people have access to personal computers. This underscores the need to consider specific populations' needs and practices when curating security and privacy advice, as well as technology design in general.

4.4.5 Concerns, Practices, and Behaviors

Security and privacy concerns When asked for any security or privacy concerns, most managers and customers were worried about hacking or online account takeover which can lead to loss of money. M13 said: *"Let's say my name is John, John something. I don't want to find another John something online. . . . If someone takes your identity, he can do so much online, tarnish your reputation, name. Yeah, so my greatest worry online I would say is identity and then my financial information, nowadays there is online banking."*

Several participants were worried about unauthorized account access. C15 stated that *"in the cyber, if you get to maybe login to, to maybe social, social websites, maybe you are going to the cyber just for a hobby or for fun, you login to a social website like Facebook, then you forget to log out of your account and then someone comes in, notices that there is an account that has not been logged out. They get to your account and post funny, funny posts, just for fun."* Other concerns included a worry about leaving data in the cybercafe that can subsequently lead to data theft. Some customers were worried about accidentally saving their passwords in the cybercafe computers as well as being shoulder-surfed in the cafe.

Concerns about customers About half of the managers indicated being worried about their customers accessing pornography or illegal sites at their cybercafe. M11 said that *"sometimes people may use sites they are not supposed to for example downloading music when we have no license for this, or access pornography."* Some managers were worried about theft of their equipment as well as scams or identity theft targeting their customers. M05 said that sometimes a *"client comes, familiarizes with the stuff. Maybe someone downloaded a CV and left it there. So this client comes, the CV has contacts for the other client and the person says: can we meet somewhere? So this client uses that opportunity to steal from the other person saying: I am an employer, I found a CV, when he's not."*

Cybercafe standard practices To protect their customers as well as to avoid legal liability, several managers indicated that they log the customer out of logged-on accounts and delete any documents or information left on the computer at the end of a customer's session. Some managers clear downloads because of space constraints while others check browser history to see if the customer accessed anything illegal. Several managers also indicated that they have physical partitions at the cybercafe for customers' privacy, while others block certain websites as well as USB drives to protect their computers from any viruses. Other precautions include having warning signs in the cybercafe to deter people from accessing illegal sites as well as disabling downloads.

Operating system updates About half of the cybercafe managers regularly or automatically update the cybercafe computers' operating systems to either improve the speed of the computers or access the latest features, but not for security. M04 said that they *"usually update because, before updating the machine, it goes slow. After updating the machine, you see it processes faster."* Those who do not update pointed to their customers being familiar with old operating systems, for example Windows 7, or not being concerned about security. Some managers also indicated that updates often slow down computers, consume a lot of storage or data, and require reboots that are sometimes inconvenient. M14 indicated that

they *"chose to stick to Windows 7 to help my customers save time because when I compare Windows 7 with these other Windows, for operating systems, I find that there's a difference. There are some customers who really struggle using Windows 10 and the others, but when it comes to Windows 7, then they're a bit more conversant with it."*

Customer standard practices An overwhelming majority of the cybercafe customers in our study indicated that they log out of their accounts once they have finished using the computers in the cafe to prevent unauthorized access of their accounts. Two customers, however, indicated that they log out only because the cybercafes they usually visit have explicit instructions or signs requiring them to do so. C12 said that in *"some cybers, when you go in, they have some instructions, they have some instructions when you enter in the cyber. So, after using a computer, you have to sign out."*

Suggestions and additional thoughts When asked for additional thoughts at the conclusion of the interviews, a few cybercafe managers and customers suggested the need for computer training to further support cybercafe customers. M10 said that *"we need to do a computer literacy program because most of the people, like 70% of the people, they are computer illiterate. So I can recommend that we have a computer literacy program that is voluntary and free so that people can know how things are done on the computer."*

Summary Most concerns in the cybercafes center around unauthorized access of accounts that can happen when customers do not or forget to log out of their accounts. Most managers are interested in protecting their customers, and undertake several measures, including logging them out. However, as noted in Section 4.4.3, some of these measures are in tension with usability, making some managers encourage their customers to select memorable passwords and sometimes even save them in the cybercafe computers to recall them.

4.5 Discussion and Conclusion

In this study, we investigate the role of cybercafes in Kenya as well as security and privacy challenges, advice, and behaviors at cybercafes through $n = 36$ semi-structured interviews. We find that cybercafes play an important role in Kenya by enabling many people to access printing, government, and other internet services. At the same time, customers face several challenges at cybercafes, mostly relating to general computer usage, account creation, and password management. Often, customers rely on the cybercafe managers for assistance when navigating these challenges. In this section, we discuss other themes that emerged from our study alongside their implications.

4.5.1 Role of Cybercafes in Kenya

Cybercafes play a crucial role in the majority world as a public location to access printing, government, and other internet tasks. In Kenya, particularly, where the government recently transitioned to an eCitizen [39] portal for most government services, customers rely on cybercafes to access these essential services, as a majority of them do not own personal computers or printers [25]. At the same time, their lack of experience with computers often causes unanticipated challenges. For example, challenges with typing and general usage of computers usually translate to difficulty selecting and remembering passwords for accounts, subsequently leading to users getting locked out of their accounts. This suggests the need for computer training to improve these users' computer knowledge and skills, as well as a need for security awareness to protect their information. As the Kenyan government is trying to digitize all its services, we believe that it should also lead these training efforts. Such initiatives should focus on the cybercafe managers who can then transfer the knowledge to their customers. Updates to the education curriculum to promote computer skills and security awareness at school could also provide long-term benefits.

4.5.2 Reliance on Cybercafe Managers

Similar to refugees' reliance on their case managers in the United States [145], cybercafe customers in Kenya significantly rely on managers for assistance setting up and managing their digital accounts. As some of these customers are novices and may have never used computers, they let the managers select and sometimes manage their passwords. Since managers have to assist several customers, they resort to techniques that help them and their customers remember these passwords, including the use of customers' ID numbers or names as passwords, writing down their customers' passwords, or using the same password for all customers. As none of the managers or customers in our study explicitly mentioned using password managers, there is an opportunity for more awareness about how password managers could assist. Phone-based password managers are promising and could be used in generating and recalling strong and unique passwords for these users as a majority of them own mobile phones. However, their device-sharing practices must be appropriately considered, and can be explored further in future research.

4.5.3 Security-Usability Tradeoff

When asked for their top advice for staying safe online, both cybercafe managers and customers often mentioned strong passwords for accounts. At the same time, most managers select or advise their customers to use passwords they can more easily remember, for example their names, children' names, ID numbers, or some combination of these, instead of choosing a strong, random password. While some managers believe such combinations make these passwords difficult to guess, the fact that the same advice is often provided to multiple customers means that customers could know other customers' passwords if they gained some personal information. Further, mobile money services such as M-Pesa [74], which are widespread in Kenya, require ID numbers of customers for transactions. It is also common for ID numbers to be recorded when visiting offices in Kenya. This means that users' passwords may be inadvertently exposed. One way to minimize such risks is for

systems including eCitizen to use passwordless authentication with phone numbers whereby users receive a OTPs for every login. This way, users would only need their phone numbers to authenticate. SMS-based two-factor authentication could also be used to improve security. Another potential workaround is for the managers to create random and unique passwords for their customers and write them down for them to keep. However, any such efforts must encourage the customers to protect their written-down passwords to be effective.

4.5.4 Security and Privacy Advice in Non-Western Contexts

One of our goals was to compare security and privacy advice in Kenya to the advice that has been extensively explored in Western contexts [23, 71]. While some of the advice including strong and unique passwords across accounts is considered important in both contexts, the most common advice in Kenya centers around the use of shared or public devices for Internet access, including logging out of accounts and not saving passwords in the browser on public computers. Our work supports the growing body of research [15, 27, 73, 130, 139] that has shown security and privacy to vary in different countries and contexts. Exploring the relevance, efficacy, and perceived actionability of existing security and privacy advice in non-Western contexts (especially for users that rely on public computers) is a promising direction to further support and protect broader populations.

OS Updates About half of the cybercafe managers in our study regularly update the cafe computers' operating systems, while the other half do not. Those that update do so to improve the performance or speed of the computers and to get new features, not because of security. Those that do not update indicated that customers are familiar with old operating systems or they are not concerned about security. Some managers pointed to updates slowing down the computers or consuming a lot of storage, data or time as reasons for not updating, similar to some of the findings of Houmz et al. [69] and Luo and Warford et al. [91]. This suggests an opportunity to communicate the role of security updates in protecting cybercafe

computers' and customers' information. In their study of users' decisions to use or not use a secure lockscreen, Albayram et al. [8] found that that a lack of risk awareness often results in insecure behaviour. Future work can therefore explore strategies to effectively communicate security risks to cybercafe managers and other users in general to encourage more secure behaviour, including regularly updating their devices' operating systems.

4.5.5 Cybercafe Risks and Concerns

Despite their obvious benefits, cybercafes can also unfortunately enable crime, illegal activities, and Intimate Partner Violence (IPV). While all the managers we interviewed indicated they do not offer illegal services, for example certificate forgery, music downloading, or activities that can enable IPV, like accessing partners' accounts, it may be the case that some unscrupulous managers may provide such services if financially motivated. One customer even expressed concern about children getting exposed to pornography at these facilities. While it is difficult to deter all cybercafes from indulging in such activities, it is still worthwile to educate managers about the dangers of these activities. The use of warnings and other notes in the cafe discouraging or prohibiting illegal activities is promising, with some customers in our interviews revealing they follow them. Nevertheless, future work can explore interventions to prevent or limit such activities from happening at cybercafes.

Table 4.3: Cybercafe Managers' and Customers' Top Three Advice for Staying Safe Online.

Code	Freq.	Sample Participant Quote
logout	12	"When you log in to a computer using your account, always log out after you've finished what you're doing in your websites, log out and delete your account." – M09
avoid-malicious-sites	11	"I just avoid clicking on links I don't know about; if those links have asked for information about yourself, you just avoid giving." – C02
strong/secure-passwds	10	"Ensure that passwords are symbols, letters and alphabets . . . and numbers. Have a mix of these so that it's not plain and avoid using things like date of birth and pet names." – C08
don't-save-passwds	9	"When you login, for example on Facebook, when the browser asks you that they need to remember your password, always click on, never, never remember the password." – C15
use-a-password	6	"Protecting accounts using passwords majorly." – M06
don't-share-passwds	5	"I don't give out my passwords, I don't share my passwords with people." – C02
avoid-public-wifi	4	"Try as much to avoid public WI-FI, somebody can easily access my work if I use a public WI-FI. So I normally try and use private internet access." – C01
unique-passwords	4	"Using different passwords on different sites." – C21
firewall	3	"Have a firewall." – M01
multifactor-auth.	3	"You should use multiple ways or multiple methods like two-factor authentication." – M03
clear-history	3	"Delete the history of your browsing because at times you might download documents and if you don't delete history, then you will be endangering your information." - C19
being-aware	3	"Being aware of recent CVEs; what happened and what you are supposed to do." – M10
delete-downloads	2	"Make sure that you clear your information when you're using a cyber because . . . someone else will be coming and if you leave information there, they may use it to do something bad." – C11
use-safe-browser	2	"Using a safe browser, I like using Brave because it blocks many pop-ups." – M13
anti-virus	2	"If you're using a laptop, the anti . . . Those software that protect any kind of virus." – C04
avoid/skip-ads	2	"I couldn't advise anyone to ever open the popping advertisements on top of the screen." – C09

Each quote can be assigned multiple codes. Only codes mentioned by 2 or more people are shown.

Chapter 5: Security and Privacy Advice in Nine Majority World Countries

This chapter goes beyond Kenya to detail our research on security and privacy advice in the majority world, including the concerns addressed by the advice. Security and privacy advice particularly plays a crucial role in how users learn how to stay safe online. However, existing research on security advice has mostly focused on Western populations [50, 125, 128, 129], and little is known about where users in the majority world get advice from and the impact of this advice on their security and privacy. To fill this gap, we conducted semi-structured interviews ($n = 70$) with "local experts" — including cybercafe operators, tech repair shop owners, teachers, phone sellers, among others — from nine majority world countries. In this work, we begin by interviewing local experts to broadly explore the security and privacy concerns and advice that local experts prioritize when supporting their local constituents; we will directly interview end-users themselves in future work.

Our study surfaces advice prioritization challenges in the majority world due to the variety of security and privacy advice offered. While the advice that local experts provide to their constituents mostly matches the advice they prioritize for their own security and privacy and advice from the West, users face significant barriers in implementing advice, including not knowing benefits of following advice (e.g., no visible UI changes after security updates), economic constraints (e.g., inability to afford expensive authentic software), and social frictions that are caused by taking protective security and privacy measures such as using a password on a phone. Further, while local experts detailed several concerns for themselves and their constituents, including fears about account compromise, misuse of personal information, financial scams, among others, we find that most of the advice they prioritize is aimed at tackling account compromise, potentially leaving them and their constituents vulnerable to the other risks. We share design interventions and argue that more work in the majority world is needed to design solutions that can protect users globally.

This chapter is based on work that will appear at the 47th IEEE Symposium on Security and Privacy [106]. I have permission from my coauthors and publishers to use this work in my dissertation. Copies of all copyright permissions are in Appendix D.3.

- Collins W. Munyendo, Veronica A. Rivera, Jackie Hu, Emmanuel Tweneboah, Amna Shahnawaz, Karen Sowon, Dilara Keküllüoğlu, Marcos Silva, Yue Deng, Mercy Omeiza, Gayatri Priyadarsini Kancherla, Maria Rosario Niniz Silva, Maryam Mustafa, Abhishek Bichhawat, Francisco Marmolejo-Cossio, Elissa M. Redmiles, and Yixin Zou. "I Wonder if These Warnings Are Accurate": Security and Privacy Advice in Nine Majority World Countries. To Appear in Proceedings of the 47th IEEE Symposium on Security and Privacy, San Francisco, CA, USA. May 2026.

Alongside Veronica Rivera, Elissa Redmiles, and Yixin Zou, I brainstormed and came up with the idea for this project. Afterward, I led the design of the interview protocol and performed the initial pilots. I collected the data in Kenya, and coordinated with my other coauthors to collect data in their respective countries, including translation and transcription. I led the data analysis and wrote the manuscript. My co-authors provided a lot of feedback throughout the research process, from ideation to the writing of the manuscript.

5.1 Introduction

Security and privacy advice plays a critical role in how users learn to stay safe online [125, 126]. Prior work shows that users get advice from various sources, including the web [128], social media [16, 21, 38, 144, 175], entertainment media [50], and friends and family [51, 65, 67, 110]. However, the wide variety of advice and perceived inconvenience of following the advice makes it difficult for both experts and non-experts to prioritize advice to follow [23, 71, 128]. Further research has shown that advice sources and willingness to follow advice are strongly influenced by the perceived trustworthiness of advice [127], convenience/security trade-offs [7, 41], and socio-demographic factors [30, 72, 125, 126, 172].

While most of this work has focused on Western users, internet users outside the West have unique security and privacy needs due to different cultures [136], infrastructure [103], and socioeconomic backgrounds [102, 126]. Thus, we hypothesize that security and privacy advice developed in the West is likely to fail when used in other places in the world, potentially leaving users at risk. For instance, while using two-factor authentication is a commonly suggested advice [23, 71], cultural expectations in South Asia dictate that women share their phones with other family members, rendering this advice impractical [136]. Similarly, to protect accounts, users are often encouraged to select strong and unique passwords across accounts [23, 71]. However, my previous cybercafe work in chapter 4 [103] finds that people often rely on public computers, e.g., at cybercafes, and the managers at those facilities to manage their passwords. To ease their workload in helping many users remember passwords, cybercafe managers encourage users to select simple passwords such as their names or ID numbers, contradicting advice from the West [23, 71].

To create a safe online experience for people in the majority world,[1] it is imperative to investigate how they are advised to stay safe and gaps in the provided advice. Prior work in Western [125] and majority world contexts [63, 67, 103] finds that people rely on others for security and privacy advice. These trusted sources include friends and family [63, 67], work colleagues [63], and community figures like cybercafe owners [103]. Our study examines security and privacy advice in the majority world through the perspectives of "local experts" i.e., individuals who offer tech support or guidance within their communities, including cybercafe operators, phone and computer repair technicians, communication technology trainers, digital freelancers, tech-savvy teachers, among others. We particularly seek to address the following three research questions:

RQ1: What security and privacy advice is prioritized by local experts in the majority world?

RQ2: What are the sources of this advice and what concerns inform the advice provided?

[1] Majority world refers to the countries that contain the majority of the world's population, and has been proposed to describe countries in Africa, Asia, and South America. It's an alternative to terms such as "developing countries" and "third world" which might come across as being pejorative.

RQ3: What barriers do local experts and their constituents face in implementing the advice?

To answer these questions, we conducted 70 semi-structured interviews with local experts in a variety of occupations, e.g., cybercafe operators, tech repair shop owners, teachers, and computer and phone sellers (more details in Table 5.2). We focus on local experts because they assist a broad range of people in their communities, providing a first look at the security and privacy concerns community members raise and the advice these experts offer them. The local experts we interviewed are from nine majority world countries spanning four continents: Africa (Ghana, Kenya, and Nigeria), Latin America (Brazil and Mexico), Asia (China, India, and Pakistan), and the Middle East (Türkiye). Collectively, these nine countries account for close to 50% of the world's population [181], and are highly diverse in their geographic locations, internet penetration rates, smartphone ownership rates, internet freedom, cultures, religion, and gender (in)equality rates (see Table 5.1).

Our study surfaces advice prioritization challenges in the majority world due to the broad range of security and privacy advice offered, similar to prior work in the West [71, 128]. While the advice that local experts provide to their constituents mostly matches the advice they prioritize for their own security and privacy, we find some differences. For instance, while local experts use VPNs, they advise their constituents to use trusted experts and memorable passwords. When we compare local experts' advice to advice from the West, we once again find significant overlap but with notable differences. For example, password managers and regular software updates are frequently encouraged in the West, but less so by local experts in our study. Importantly, users face significant barriers in implementing advice, including not knowing benefits of the advice (e.g., no visible UI changes after security updates), economic constraints (e.g., inability to afford authentic software), and social frictions that are caused by taking protective security and privacy measures such as using an unlock PIN or password on a mobile phone.

While prior work has quantified correlations between sociodemographic factors and security and privacy practices [174], our study contributes in-depth insights into *how*

gender, culture, and religion shape security and privacy concerns and advice in the majority world. For instance, collectivist cultures and religion compel people to share their devices, undermining privacy affordances from the West where device sharing is less common. Gender influences advice-seeking behaviors, with women preferring to seek advice from other women. Our work suggests the need for better advice prioritization and consideration of majority world users in tech and security and privacy design. We also advocate for better translation of tech tools and security and privacy advice. Lastly, our methodology shows how and why it is critical to engage local communities in conducting similar research.

5.2 Methodology

To explore security and privacy advice across nine majority world countries, we worked with local in-community contacts and collaborators to identify and interview 70 local experts. We chose interviews because (i) our research questions are exploratory, and interviews allowed deeper probes; (ii) many of the countries we focus on lack survey infrastructure and are not covered by survey platforms such as Prolific.

5.2.1 Country Selection

We selected nine majority world countries that are highly diverse in their geographic locations, internet penetration rates, smartphone ownership rates, internet freedom scores, cultures, religion, and gender (in)equality (see Table 5.1). Prior work [103,126] suggests that these factors influence peoples' security and privacy concerns and practices. In particular, we selected countries from the following regions: Africa (Ghana, Kenya, and Nigeria), Latin America (Brazil and Mexico), Asia (China, India, and Pakistan), and the Middle East (Türkiye). On aggregate, these nine countries account for approximately 47.48% of the world's population [181] but remain understudied in security and privacy research [61].

Table 5.1: Factors That We Considered in Selecting the Nine Majority World Countries.

Country	Region	Pop. Size [181]	Internet Pen. [36, 180]	Smartphone Ownership [150]	Internet Freedom [49]	Gender Ineq. [163]
Kenya	East Africa	56.4M	29%	53%	68%	0.506
Nigeria	West Africa	232.7M	55%	38%	57%	0.680
Ghana	West Africa	34.4M	68%	50%	65%	0.512
Mexico	Latin America	130.9M	76%	62%	61%	0.309
Brazil	Latin America	212.0M	81%	67%	65%	0.390
China	East Asia	1.419B	88%	72%	10%	0.168
India	South Asia	1.450B	46%	47%	51%	0.490
Pakistan	South Asia	251.3M	21%	31%	26%	0.534
Türkiye	Middle East	87.5M	81%	75%	32%	0.638

5.2.2 Research Personnel

To execute this large-scale study across multiple countries, we started with a core multi-disciplinary team of five researchers. The core team has vast experience studying security and privacy in both Western and majority world countries, as well as engaging with at-risk populations. Three members are natives from two majority world countries, and the core team collectively speaks four languages spoken in the countries of study. After the core team ideated and designed the study, we expanded the team's diversity in lived experience, expertise, and language skills by building and collaborating with a distributed network of 13 additional researchers and contacts in the nine majority world countries. Our local contacts helped us identify and recruit suitable participants and conduct interviews in local languages.

We compensated our local contacts for their assistance in translating the interview protocol, moderating the interviews, and delivering the transcripts in English. We also included as coauthors all our contacts who engaged in data analysis and paper writing. For quality control, our core team reviewed all prospective participants shortlisted by the local contacts to ensure they matched our criteria for local experts prior to conducting interviews. For our contacts new to qualitative research, the core team trained them on how to effectively conduct interviews. We also invited them to listen in on interviews conducted in other countries. Where language permitted, a member of the core research team also participated

in interviews conducted by our local contacts and asked follow-up questions where needed.

5.2.3 Recruitment and Demographics

We define a local expert as anyone who provides tech (or related) services, support, or advice to members of their community. While prior work in the majority world has used terms like intermediaries [137] to describe individuals who assist others with technology, we use the term local experts to specifically refer to those who are frequently consulted and regarded as knowledgeable, often outside of the familial relationships typically associated with intermediaries. To meet our criteria, these experts had to be publicly-facing and directly supporting the general public regularly as part of their job. Their job roles can include tech/repair shop owners, operators at cybercafes or libraries, phone/sim card sellers, teachers, religious leaders, community leaders, and more.

As local expert profiles can vary across countries, we worked with local contacts to identify and recruit suitable participants who met our criteria. Working with local contacts helped us reach populations (e.g., indigenous communities in the case of Mexico) that would otherwise have been impossible to reach. We did not publicly advertise the study to avoid scammers attempting to participate without meeting our criteria [116]. Additionally, as the interview protocol touches on sensitive topics such as surveillance, we wanted to avoid attracting scrutiny from officials in countries with authoritarian regimes to minimize risk to participants. In the end, we recruited a diverse pool of 70 local experts across the nine majority world countries, with each country having at least five and up to ten experts. Table 5.2 has more details about local experts and their roles.

5.2.4 Interview Procedure

We developed our interview guide around our research questions. Below is a summary of the interview procedure (see Appendix C.1 for the full protocol).

Table 5.2: Demographics of the Local Experts in the Nine Majority World Countries.

ID	Country	Area	Age	Gender	Education	IT Back.	Local Expert's Role in their Community
P01	Kenya	Urban	40	Woman	Form Four	No	Sells electronic devices including phones.
P02	Kenya	Rural	37	Man	Diploma	Yes	Owns and operates a cybercafe.
P03	Kenya	Both	30	Woman	Bachelors	Yes	Operates a tech repair shop.
P04	Kenya	Urban	30	Man	High school	No	Sells phones, SIM cards, and other accessories.
P05	Kenya	Urban	25	Woman	Diploma	Yes	Works at Huduma Center (a government ICT center).
P06	Kenya	Semi	29	Woman	Bachelors	Yes	Owns a cybercafe and teaches ICT at a high school.
P07	Kenya	Both	33	Man	Masters	Yes	Owns and has previously worked in a cybercafe.
P08	Kenya	Urban	33	Man	Diploma	No	Works at a local cybercafe.
P09	Kenya	Urban	28	Man	Bachelors	Yes	Works at Huduma Center (a government ICT center).
P10	Kenya	Rural	31	Woman	Bachelors	No	Works at Huduma Center (a government ICT center).
P11	Nigeria	Urban	_	Man	Masters	Yes	Operates a tech repair shop.
P12	Nigeria	Urban	28	Man	Masters	Yes	Sell computers and operates a tech repair shop.
P13	Nigeria	Urban	_	Woman	Masters	Yes	Works at a cybercafe.
P14	Nigeria	Urban	28	Woman	Bachelors	Yes	Graphics design, and owns an ICT training center.
P15	Nigeria	Urban	_	Man	Masters	Yes	Sale and repair of tech, and software installation.
P16	Nigeria	Rural	28	Man	Bachelors	Yes	Works at a cybercafe.
P17	Nigeria	Urban	_	Man	Bachelors	Yes	Performs website design and owns a cybercafe.
P18	Nigeria	Rural	23	Man	Bachelors	No	Multimedia designer and a digital services consultant.
P19	Nigeria	Urban	_	Woman	Masters	Yes	Typing, printing and computer training.
P20	Nigeria	Urban	30	Woman	Bachelors	No	Runs a cybercafe, performs data entry and analysis.
P21	Ghana	Rural	38	Man	Diploma	Yes	Works at a cybercafe.
P22	Ghana	Urban	25	Man	High school	No	Manages and operates a cybercafe.
P23	Ghana	Urban	24	Man	High school	No	A graphic designer and IT technician.
P24	Ghana	Rural	20	Man	High school	Yes	Provides community tech support and assistance.
P25	Ghana	Urban	36	Man	Masters	Yes	PC and printers technician.
P26	Ghana	Urban	43	Man	Bachelors	Yes	A teacher, performs phone repairs and sales.
P27	Ghana	Urban	24	Man	Bachelors	Yes	Computer sales, repair and software installation.
P28	Ghana	Rural	_	Man	Bachelors	No	Works at cybercafe, and serves as a printing manager.
P29	Ghana	Semi	44	Man	Masters	Yes	Teacher and a manager at a cybercafe.
P30	Ghana	Rural	43	Man	Bachelors	Yes	Works at cybercafe, and serves as a printing manager.
P31	Mexico	Rural	38	Man	Bachelors	Yes	Teacher that people consult with concerns about tech.
P32	Mexico	Rural	42	Woman	Bachelors	Yes	Teacher, owns cybercafe, and sells and repairs tech.
P33	Mexico	Rural	38	Man	_	Yes	Computer repair technician.
P34	Mexico	Urban	29	Man	Bachelors	Yes	Civil servant who works with rural communities.
P35	Mexico	Urban	33	Woman	Bachelors	Yes	Only woman in her region that owns a cybercafe.
P36	Mexico	Rural	47	Man	Masters	No	Teaches computing at primary school, and does repair.
P37	Mexico	Urban	40	Man	Bachelors	Yes	Works in IT and has offered his services to rural areas.
P38	Brazil	Urban	43	Man	Technical	Yes	Teaches computing to people with limited knowledge.
P39	Brazil	Urban	19	Man	Technical	Yes	Supports public schools e.g., software installation.
P40	Brazil	Urban	39	Man	_	_	Tech repairs, and are now authorized by Apple.
P41	Brazil	Urban	48	Woman	Masters	Yes	Refurbishes and donate computers to public schools.
P42	Brazil	Urban	21	Man	High school	Yes	Intern at a school lab, performs installation and repair.
P43	Brazil	Urban	23	Man	High school	Yes	IT mentorship at a local church, and does tech repair.
P44	Brazil	Urban	18	Woman	Technical	Yes	Teaches computer skills to people in community.
P45	Brazil	Urban	22	Man	High school	Yes	Intern at a school lab, performs installation and repair.
P46	Brazil	Urban	23	Man	High school	Yes	Tech support services at a government office.
P47	China	Urban	24	Man	Bachelors	No	Police officer and mainly handles fraud.
P48	China	Urban	51	Woman	Bachelors	No	Police officer and mainly handles fraud.
P49	China	Urban	35	Man	Bachelors	Yes	Network engineer, helps others on social media.
P50	China	Urban	34	Man	High school	Yes	Owns 12 tech repair service stores
P51	China	Urban	26	Woman	Bachelors	Yes	A network security service business manager.
P52	India	Semi	40	Man	Bachelors	Yes	Runs a cybercafe and cable business.
P53	India	Urban	58	Man	Diploma	Yes	A teacher of yoga.
P54	India	Urban	39	Man	High school	Yes	Operates a tech repair shop.
P55	India	Urban	29	Man	Masters	No	Sells mobile phones and performs repairs.
P56	India	Urban	38	Man	High school	No	Sells electronics including phones.
P57	Pakistan	Urban	34	Man	Bachelors	Yes	Owns and operates a mobile repair shop.
P58	Pakistan	Urban	38	Man	High school	Yes	Owns and operates a mobile repair shop.
P59	Pakistan	Urban	30	Man	High school	Yes	Freelancer and provides e-commerce services.
P60	Pakistan	Urban	33	Woman	Masters	Yes	Freelance and provides Amazon services to clients.
P61	Pakistan	Urban	26	Man	Masters	Yes	Freelancer and also works as a data scientist.
P62	Pakistan	Urban	22	Woman	Bachelors	Yes	Online tutor and researcher.
P63	Pakistan	Urban	31	Woman	Bachelors	Yes	A technical writer and online tutor.
P64	Pakistan	Urban	31	Woman	Masters	Yes	Social mobilizer at an NGO.
P65	Pakistan	Urban	32	Woman	Bachelors	Yes	A teacher and also sells mobile phone accessories.
P66	Türkiye	Rural	50+	Man	Associates	No	A public servant.
P67	Türkiye	Urban	26	Woman	Bachelors	Yes	Teacher and provides tech support and advice.
P68	Türkiye	Urban	21	Man	High school	Yes	Mobile phone repairs.
P69	Türkiye	Urban	45	Man	Masters	Yes	Works at a public library.
P70	Türkiye	Urban	29	Woman	Bachelors	Yes	Pharmacist but helps people access e-government.

Local experts' background We first asked local experts about their background. Next, we asked them about technology challenges in their communities, followed by the support they provide others in resolving them. We also asked about the sources of this advice.

Security and privacy concerns Our next questions focused on concerns around technology and security and privacy. We first asked local experts about concerns they have about their own security and privacy and how they handle them, followed by the concerns people in their community come to them with and how they help them resolve these concerns.

Security and privacy advice We asked experts to provide their top three pieces of advice they currently (or would) follow to protect their security and privacy, following Ion et al. [71]. We probed where they learned the advice from, if they follow the advice, and challenges in following the advice. Following, we asked the experts for the top three pieces of advice they have provided (or would) to those they support. We also asked about advice people are likely to follow and advice gaps.

Tech, and security and privacy practices and challenges Next, we asked questions about local experts' personal technology use and practices, as well as those of other people they support in their local communities. We further probed about specific potential challenges in their communities such as common scams and phishing schemes.

Other contextual factors To understand how security and privacy concerns and advice further vary, we next asked local experts whether they vary advice they provide based on their constituents' gender, religion, age, job type, as well as any other factor.

Demographic questions Lastly, we asked local experts about their demographics including age, gender, and education. We also asked them to share any feedback they had.

5.2.5 Data Collection

Due to the logistics involved in executing this study across nine countries, we started data collection in December 2023 and ended it in February 2025. We conducted pilots with two local experts, one from Kenya and another from China. We used the pilot feedback to refine our interview protocol and add more probes [28]. For example, when experts indicated they had not provided any advice, we asked them what advice they would provide if people asked. The interview guide was developed by our core team in English and translated to local languages by our contacts and collaborators. Most recruitment and interviews were conducted remotely and in local languages[2] by our collaborators, with the transcripts later translated to English for analysis. All interviews were audio-recorded. We compensated participants the equivalent of $40 based on the purchasing power parity of their countries [131]. For example, this translated to Ksh. 1,700 or $13.15 in Kenya. In some cases, we adjusted these rates as suggested by our contacts.

5.2.6 Data Analysis

We qualitatively analyzed the interview transcripts using MAXQDA [93]. First, the lead researcher (serving as the primary coder for all transcripts) coded a few transcripts from Kenya to develop an initial primary codebook. Using this codebook, five secondary coders comprising in-community contacts or collaborators from Kenya, Ghana, China, Pakistan, and Turkiye performed secondary coding in their respective countries. As this was not possible for Nigeria, Brazil, Mexico, and India, our secondary coders with geographical proximity or familiarity with the culture in these countries assisted. For example, our Pakistani contact performed secondary coding for transcripts from India. In all the countries, at least half of the transcripts were double-coded and discussed by both coders. These discussions were used to refine codes and identify emerging themes, and therefore there was

[2]As English is an official language in Ghana, Kenya, and Nigeria, interviews there were conducted in English. In Turkiye, one interview was conducted in English as the interviewee doubled as an English teacher.

no need to calculate inter-rater agreement [99].

5.2.7 Limitations

Our study has several limitations. First, our sample size per country was relatively small. In Mexico, our engagement of indigenous students to recruit participants and conduct interviews might have biased our sample toward marginalized communities. Additionally, local experts across the nine countries were very diverse, with some countries having predominantly rural experts, while others had experts based in urban areas. However, the goal of our work is not to generalize to any of the countries but to surface common concerns and security and privacy advice. We also avoid making country-level comparisons as much as possible due to the diversity of experts across the nine countries. Further, as we conducted the interviews in countries that speak different languages and have different cultures, it is possible that some phrases or nuances might have been lost in translation. To mitigate this, we worked closely with local collaborators to ensure that our interview guide was appropriately translated and that interviews were conducted in local languages. We also involved our local contacts in analyzing the data and writing the results to ensure the local context was appropriately considered and respected throughout this study.

5.2.8 Ethical Considerations

Our study was reviewed and approved by five institutional ethics review boards. Where appropriate and possible, such as in Kenya, we also obtained local ethics approval. We took several measures to protect our study participants. In particular, participation was completely voluntary — participants could opt out anytime or decline to answer any question. As some of the questions (e.g., about surveillance) might put participants at risk, we worked with our local contacts and collaborators in each country to ensure it was both appropriate and acceptable to ask these questions. On three occasions during interviews, local experts were hesitant to discuss surveillance, and we thus did not probe any further. We minimized the

collection of personally identifiable information (PII) from participants. Any PII shared by participants was removed from the transcripts before we conducted the analysis. In some cases, we collected participants' phone numbers for interview scheduling and payment; we deleted these details after interview completion.

Throughout the ideation, design, and execution of this study, we reflected on our goal for this work and made efforts to work with local collaborators from each country to ensure (a) local context is appropriately considered; and (b) research benefits can directly extend to local communities, in line with the research justice principle in the Belmont report [14].

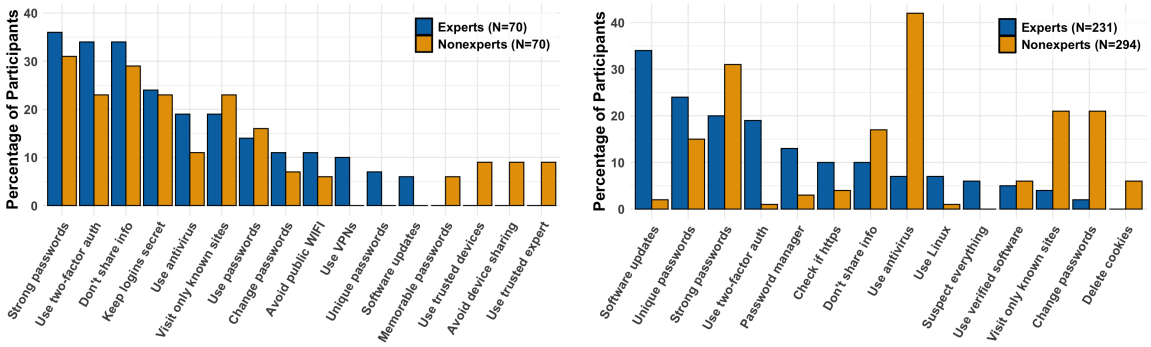
5.3 Results

In this section, we discuss local experts' top advice for their own security and privacy and that of their constituents, followed by sources of the advice. We then discuss the concerns that this advice seeks to address and the reasons why both local experts and users follow the advice. Lastly, we discuss barriers and contextual factors that make it challenging for users to follow the advice. We refrain from reporting counts to avoid implying generalizability; those provided in Figure 5.1 show how the advice in our study compares to prior work; however, we caution against drawing any generalized findings. Finally, we focus on broader themes across the nine countries, and where possible, mention some country-specific themes.

5.3.1 Top Three Security and Privacy Advice

Overview While the advice in our study overlaps with advice from the West — evidenced by the use of strong passwords and two-factor authentication — we also found several differences. For example, local experts often promoted general password use (including memorable passwords) among their constituents, prioritizing account access over security.

Top security and privacy advice Figure 5.1 shows participants' top three advice for staying safe online. Figure 5.1a has advice mentioned by local experts (n=70) in our study



(a) Top advice from our study.

(b) Top advice from Ion et al. [71]

Figure 5.1: Top Advice for Staying Safe Online. Note: Figure 5.1a has advice from our study while Figure 5.1b has advice from Ion et al. [71]. Since we only interviewed experts in our study, both expert and non-expert advice in Figure 5.1a was from experts' perspectives.

for their security and privacy (experts) but also that of their constituents (nonexperts), while Figure 5.1b has the top advice mentioned by both experts (n=231) and nonexperts (n=294) in an earlier US-based survey study by Ion et al. [71]. While Busse et al. [23] recently replicated the study by Ion et al. in Europe, we compare our results only to the original work by Ion et al., as the findings from Busse et al. overlap with those of the original study.

Expert vs. non-expert advice in the majority world Overall, we find that local experts' top three personal advice for staying safe were mostly similar to the top three advice they provide to their constituents (Figure 5.1a). This advice revolved around the use of strong passwords, 2FA, not sharing personal information, keeping logins secret, using anti-virus software, avoiding clicking on unknown links, generally using passwords, frequently updating passwords, and avoiding public WI-FI. However, we also noted some differences. In particular, experts themselves additionally seemed to use VPNs and prioritize software updates, but less frequently recommended this advice to others. It appears that when advising others, experts prioritize advice that is simple for users but also affordable. Unfortunately, as software updates often require purchasing the Internet, this can often be seen as unnecessary cost for users, especially if they do not understand the benefits of the updates.

On the flipside, experts encourage their constituents to use trusted devices, avoid device sharing, consult trusted experts only, and use memorable passwords more compared to their own personal advice. We hypothesize that because users often need to share their sensitive data for assistance, local experts emphasize the need for trust, both on the device level as well as for consulted experts. For passwords, local experts recommend memorable passwords because their advisees frequently forget complex passwords. Thus, account access is often prioritized over account security.

Advice in the majority world vs in the West When we compare advice from our study (Figure 5.1a) to Ion et al.'s (Figure 5.1b) study, we find many similar pieces of advice, but with some differences. Strong passwords, unique passwords, use of 2FA, use of anti-virus, frequent password updates, avoiding unknown links, and not sharing personal information appear in both studies. However, the use of password managers is recommended frequently by experts in Ion et al, but not by experts in our study at all. This suggests that users (and even local experts) in the majority world might be less familiar with password managers. While software updates are the most frequently mentioned advice by experts in Ion et al.'s study, this advice is mentioned less frequently in our study. We hypothesize that local experts in the majority world might not really view the security benefits of these updates as a priority. Internet costs might also make them less likely to recommend this advice.

On the flip side, experts in our study frequently mention the use of passwords, avoiding public WI-FI, and regular backups; these are not among the top advice mentioned in Ion et al.'s study. While backups are a great piece of advice, using passwords alone is not sufficient for account security, especially if the passwords are weak, reused, or saved on shared devices. Avoiding public WI-FI is no longer important today, given that many websites have switched to using HTTPS. At the same time, however, local experts and their constituents do not always follow these pieces of advice, and we discuss reasons for that later in Section 5.3.5.1.

Main takeaway Local experts in the majority world tailor their security and privacy advice to the practical needs of their constituents, prioritizing usability, account access, and affordability over strict adherence to "security best practices." Practices that are deemed costly, complex, or resource-intensive (e.g., software updates or VPNs) may be personally adopted by local experts but are not provided by local experts to their constituents. This directly shows how infrastructural and economic constraints shape security and privacy advice and practices in the majority world.

5.3.2 Sources of Advice

Overview While sources of advice such as online platforms, past negative experiences, formal training, social circles, and traditional media have also been documented in Western contexts, we find that community ICT centers play a significant role in providing tech advice and support in the majority world. Additionally, many experts note a growing reliance on children as a trusted source of digital guidance.

Online sources Similar to prior work in the West [21, 140, 144, 175], local experts across the nine majority world countries overwhelmingly pointed to online sources, including online searches and social media, as a source of advice for themselves and others in their communities. Different from those studies, some local experts indicated running social media pages, e.g., on Facebook as well as WhatsApp groups, to disseminate advice to their constituents. P56 (India) indicated that *"the Internet has all the answers these days"* while P02 (Kenya) runs *"several Whatsapp groups where I update them [people in their community]."* P58 (Pakistan) was overly trusting of advice on the Internet, stating that *"the Internet can not lie to you.* However, P41 (Brazil) was skeptical, stating that for their *"family, sometimes they share something in WhatsApp groups, and we say, no, it's not like that, you have to look for more reliable source[s] information.*

Previous negative incidents Similar to prior work in the West [121, 125], we find that previous negative incidents are a common source of advice. For instance, P04 (Kenya) uses strong passwords because *"a friend was using simple passwords and somebody came and guessed his information/passwords and entered into his accounts and messed up everything."* Regarding keeping logins secret, P55 (India) *"learned this from the mine and customers' experiences that we've had to deal with."* P44 (Brazil) *"learned the importance of backups through personal experience . . . This lesson hit home when I uninstalled WhatsApp while formatting my phone, not realizing I needed a backup, and ended up losing everything."*

Formal training Similar to Redmiles et al. [125], some local experts pointed to some formal training as a source of their advice or expertise. This ranged from IT-related courses in school to courses taken online. For example, P23 (Ghana) *"was first introduced to VPN[s] by my teacher . . . in high school"* while P44 (Brazil) *"learned about this [keeping passwords secret] in my technical course."*

Social circles Another common source of advice for experts and their constituents was friends, partners, family, and colleagues, similar to previous work in the West [125]. In our study, however, local experts detailed how people increasingly rely on their children for advice. For instance, P55 (India) stated that people usually *"ask people around them, children around them, or someone who might be technically sound in their neighborhood."* Similarly, P67 (Türkiye) mentioned that parents rely a lot on their children: *"I think parents also use their children's, uh, support to . . . navigate through technology because our day and age children are really good."* The reliance on children for advice suggests that updates to school curriculum in the majority world to cover technology and security awareness could have widespread impacts.

Community ICT centers Different from prior work in Western contexts [125], some experts pointed to local community ICT centers as places where people in their local

communities seek advice or tech support. This included libraries (Türkiye), tech repair shops (Pakistan, Türkiye, Brazil, Ghana, Kenya), cybercafes (India, Kenya, Mexico), churches (Brazil), phone and computer sellers (Brazil, Ghana), government ICT centers (Kenya), and pharmacies (Türkiye). For example, P63 (Pakistan) stated that *"in Pakistan, it's very common to go to phone-repair shops to get technology support."* P43 (Brazil) pointed out how local churches also play an important role: *"The pastor . . . makes an ad about it, saying that on such and such a day, at such and such time, there will be a class, there will be a course for people to learn about computing."*

Official sources While official sources are used more by users with more resources in the West compared to those with fewer resources [126], only a few experts in our study pointed to official sources, including customer care and government websites. While official sources are authoritative, users are hesitant to use them because of cost constraints. P11 (Nigeria) stated that there are *"premium services like people who go to Carlcare which are like the official companies/service representatives and so some people go to them because they believe that what comes for them is satisfactory."*

Traditional media Lastly, a few experts mentioned getting advice from traditional media sources, including radio and TV. For example, P30 (Ghana) learned to avoid *"suspicious link[s] through education on the TV [and] on the radio"* while P44 (Brazil) said that *"in small towns, radio is still a big deal."* For rural areas in the majority world, traditional media could especially be a useful way to disseminate advice.

5.3.3 Concerns Addressed by Advice

Overview We now discuss concerns that influence security and privacy advice provided by local experts. While most concerns, including account compromise and financial scams, have also been noted in the West, we find that most of the advice provided by local experts (see Section 5.3.1) protects users against account compromise, but less so against other

concerns such as stalking and intimate partner violence. This potentially leaves users vulnerable to other security and privacy risks.

Account compromise Described as "hacking" by local experts, account compromise occurs when an unauthorized individual gains access to a user's account [40, 168], allowing them to impersonate or take over the account. Throughout our study, local experts frequently mentioned account compromise — especially for social media accounts like WhatsApp and Facebook — as a concern for themselves and their constituents. P06 (Kenya) worried that *"we have hackers everywhere these days"* while P12 (Nigeria) mentioned that *"people complain to me that their social media accounts have been hacked, especially WhatsApp."*

Account compromise occurs in various ways, e.g., users forgetting to log out of public computers, inadvertently sharing one time passwords (OTPs) with attackers, or clicking on phishing links. P22 (Ghana) shared: *"Someone can guess your number and then try to log into your WhatsApp, but then you will surely receive a message and they will call you to ask you for a code. And when you mention the code to them, they get into your WhatsApp."* While experts shared ways to mitigate account compromise including not sharing OTPs or avoiding unknown links, they also mentioned that some users are unconcerned about account compromise, choosing to simply create new accounts, as elaborated by P38 (Brazil): *"The person says, okay, you hacked my social network, no problem, I'll create another account."*

Misuse of personal information While account compromise involves unauthorized parties getting access to users' data, participants also worried about authorized parties using their data for purposes other than legitimate ones. P38 (Brazil) argued that *"there is no free lunch . . . all the applications that come for free have as a goal to watch us."* P44 (Brazil) was worried about their information being used for advertisements: *"If an app is free to . . . use, it means you're paying with your data in some way . . . They might not steal your data, but they do collect certain information and sell it to other apps."* This was echoed by P07 in Kenya, where mobile money is common: *"We mostly pay our bills using mobile phones*

but you find later those people whom you paid those funds they call you back like they are advertising their services . . . something that you never consented to." While prior work in the West also notes privacy concerns, e.g., with online ads [183, 184], our results show how emerging technologies in the majority world, such as mobile money, introduce new privacy risks for users, suggesting design opportunities to improve the privacy of these technologies.

Financial scams Financial scams are deceptive methods used to steal money from people [35]. Local experts were worried about financial scams targeting themselves and their local constituents. P54 (India) was concerned that *"a lot of scams are happening these days."* P49 (China) described two scenarios: *"In one, they've [people in their community] already been scammed and are stuck in an endless loop of transferring money, unsure of whether to continue. In the other, they're being blackmailed and don't know how to handle it."* In most cases, social engineering [173] is used to trick victims as detailed by P06 (Kenya): *"I have a lady who was conned 2 million at Standard Chartered Bank and she was called by someone and they told her your account has some issues kindly give us your date of birth, your last transaction and the numbers they use are close to the actual numbers of the bank."*

Malware Malware is malicious software designed to harm devices or data [153]. Because of the nature of websites they access, many local experts were concerned about viruses infecting their devices or those of people in their local communities. For instance, P69 (Türkiye) stated that they are *"interested in sports. I look at Fotomaç newspaper every day. You know, in order to look at a page there, maybe 10 or 15 advertisements come from there. Maybe you can get a virus."* This was echoed by P62 (Pakistan) for movies: *"There are websites where I usually go to watch certain shows. So I know for sure that, you know, there are a lot of things that can go wrong here, but there are no other options in Pakistan."* Similarly, P47 (China) said: *"When downloading certain apps . . . my phone's security system sometimes warns me that the app might have risks, like viruses or potential data breaches. But* ***I wonder if these warnings are accurate.*** *Despite the warnings, sometimes*

I have no choice but to download the app to complete a task." Similar to prior work with refugees in the US [145] and loan app users in Kenya and India [102, 122], our results show how users de-prioritize security and privacy when faced with competing priorities. This is exacerbated by low socioeconomic conditions in the majority world.

Social harms Social harms are the collective negative effects of behaviors or actions on an individual, community, or society [100]. Local experts were worried about the negative impact of access to pornography and gambling — made easy by technology — on their communities. P15 (Nigeria) worried that *"one of the things that technology has done, especially for young children, is it has made them addicted to technology and they have pornography and that sort of thing. And it has really made a lot of youths not focus on their education."* When doing repairs, P25 (Ghana) described how *"a lot of people . . . have pornography on the laptop . . . so some time you try to do back up for them [before repair] and when you go to the camera you will see things that you shouldn't see."* P58 (Pakistan) was worried that TikTok *"is mostly used to promote obscenity and vulgarity"* while P43 (Brazil) was concerned about gambling: *"I believe this is very harmful for people. It ends up taking their money."* We speculate that concerns around social harms might be more pronounced in the majority world due to collectivist values.

Intimate partner violence (IPV) IPV refers to physical or sexual abuse, stalking, and other forms of harm caused by an intimate partner [24]. Some experts recounted incidents where people in their communities had been targets of stalking via spyware and other forms of IPV. P25 (Ghana) detailed how *"most [targets] are the ladies. So what happens is that the guys will tap their WhatsApp and be reading their messages . . . one lady informed me that . . . she was beaten by her boyfriend; that she had been chatting with another man . . . So I went through the phone . . . and I asked her about many apps, but she said some were not installed by herself."* Sometimes this stalking was facilitated by device or account sharing, as elaborated by P49 (China): *"I have a friend who shares an Apple ID with his*

wife. Through the ID's tracking feature, she knows his every move." While IPV has been extensively explored in the West [24, 46–48, 157, 158, 185], we note that factors like low digital literacy in the majority world make targets more vulnerable.

Image-based sexual abuse (IBSA) IBSA occurs when someone takes, shares, or threatens to share sexually explicit images or videos of another person without their consent [171]. It can take many forms, including nonconsensual distribution of consensually-created intimate content (NDII), nonconsensual creation of the images, or unsolicited sharing [120]. In our study, local experts were worried about some forms of IBSA, especially targeting women. For instance, P39 (Brazil) mentioned that *"[female] teachers, especially, were much more concerned with image leaks, with image manipulation, than men . . . because image manipulation is a relatively new threat, is much scarier to women than to men. And, of course, women are much more targeted."* P02 (Kenya) was worried about NDII: *"People who use technology for very dubious reasons to gain dubious things. We have someone who uses technology to download things like porn, part of it to sell."* P32 (Mexico) shared an incident where accounts were compromised and used to distribute images, causing emotional and physical abuse: *"[Hacking] happened to a couple of young girls. One of them looked for me and told me that her Facebook profile had been hacked, they made a photomontage of her, and many people saw it, her father hit her and kicked her out of the house."* Some experts were worried about how advances in AI have made it easy to create deepfakes.

Digital surveillance Digital surveillance is the use of technology to monitor and track activities of other people [111], including their online communications. When probed about this, local experts across all nine countries believed digital surveillance exists in their countries, and is conducted mostly by governments and tech companies. Many local experts and those they support were worried about this surveillance. For instance, P43 (Brazil) said: *"Some people do worry and are afraid of being watched. It even happens that people say something, and shortly after, they see advertisements related to what they talked about."* P36

(Mexico) added: *"There are people I have heard who believe that we are watched by the government or other non-governmental institutions and that we should be careful."*

Despite these concerns, many experts felt helpless in avoiding surveillance because they could not avoid using technology or because the government is too powerful. Regarding the government, P67 (Türkiye) said that *"you can't really do much"* while P49 (China) added that *"in China, it's almost impossible"* to avoid surveillance. P38 (Brazil) stated that *"it's impossible to stop being watched. Because most of the applications that we are dependent on use the application as a form of surveillance. Facebook, WhatsApp, TikTok, and so on."*

5.3.4 Reasons for Following Advice

Overview Local experts provided various reasons why they and their constituents follow recommended security and privacy advice. While reasons including knowing benefits/risks, previous negative incidents, and simplicity of advice are consistent with prior work in the West, we find that trust between experts and users is critical in the majority world.

Understanding the benefits and risks The most commonly cited reason for following advice was understanding the benefits of the advice and the risks of not following it. For 2FA, P21 (Ghana) said that *"it is important because setting up that two-step verification, no one can hack your account."* This was echoed by P67 (Türkiye) who added that *"passwords can always be breached. But two-step verification uses your phone. It's harder to be breached."* For strong passwords, P32 (Mexico) stated that *"having a secure password is an important aspect of keeping the security and privacy of your online information."*

Trusting local experts Previous work in the West [125] notes that users are more likely to follow advice if they trust the source. We extend this work to the majority world and show how local constituents trust advice from local experts because of the trust they have developed with the experts. This sometimes forces people to only seek help from certain experts, as P20 (Nigeria) recounted: *"I had a customer who wanted to print a personal*

document relating to her salary and all that, and she kept telling me that she cannot take it to any other cybercafe but mine because she trusts me." We note that trust between users and the experts is important as local experts often access sensitive information when supporting their constituents — this has also been noted for case managers and refugees in the US [145], cybercafe managers and customers in Kenya [103], and repair shop owners and customers in India [101]. Further, this trust sometimes intersects with gender, as some users trust women experts more and consult them for sensitive transactions.

Negative incidents Similar to prior work in the US [125], some local experts described previous negative incidents as a reason for following advice. P01 (Kenya) frequently changes their passwords due to *"the time someone used my password to borrow money on my behalf I felt humiliated and so I had to keep on changing."* P64 (Pakistan) protects their data because *"sometimes people use others' phones and start browsing their pictures, which is personal. I've seen people unlock phones, access contact numbers, and even extract numbers . . . So, I decided to secure my photos and numbers."* For P43 (Brazil), *"after having some of my social networks hacked, I started using MFA on almost all my accounts."*

Advice being simple Lastly, some experts mentioned that people are more likely to follow recommended advice if it is simple to implement. For example, P59 (Pakistan) stated that *"people will prefer to follow simpler advice."* Similarly, P20 (Nigeria) said that people are more likely to follow their advice of generally using passwords *"because it is easy for them to follow compared to others."* Our findings support those of Redmiles et al. [125] about the need to make security imperatives simple for users to implement them.

5.3.5 Challenges and Contextual Factors

Finally, we discuss contextual factors and barriers to following recommended advice.

5.3.5.1 Challenges to Implementing Advice

Overview While inconvenience has also been noted as a barrier for following advice in the West, we find socioeconomic factors, not knowing benefits, language barrier, and social frictions of taking protective measures as barriers for following advice in the majority world.

Inconvenience of implementing advice Prior work in the US has noted inconvenience as a reason for users rejecting advice [125]. We confirm and extend these findings to the majority world, showing how such inconveniences can stem from poor connectivity or government-imposed internet and network shutdowns in the case of 2FA. These inconveniences also lead experts to prioritize account access over security when creating passwords for their constituents. For example, P02 (Kenya) stated that *"some people still get challenges because you create a strong password for someone and someone forgets [it]."* Regarding 2FA, P59 (Pakistan) said that *"sometimes, you don't get the code when you activate two-factor authentication, or when the phone services are down in Pakistan."* These inconveniences lead to insecure practices such as reusing passwords or turning off 2FA.

Socioeconomic factors Previous work in the West notes that users of lower socioeconomic status struggle to find information on the web [59, 60, 149, 167]. Further, these users lack access to more authoritative sources of security and privacy advice [125]. We extend these findings to the majority world to show how limited finances often inhibit people from implementing recommended security and privacy advice. P27 (Ghana) highlighted how internet costs prevent people from updating their software despite knowing the benefits: *"Most of them, I think for the Internet concerns, they are not willing to update phones because update takes a lot of Internet subscriptions . . . so most of them often frequently do not update knowing fully well the importance of these updates."* P70 (Türkiye) said that they *"do not update it [their OS] . . . for financial reasons. Since this is a cost, I don't see it necessary in*

Türkiye." Similarly, P43 (Brazil) stated that *"some people lack the resources to get antivirus software"* while P44 (Brazil) added *"they'd say, but you have to pay for antivirus, why should I get it?"* In Pakistan, P61 remarked that most people *"don't even try to spend their money on VPN. No one pays attention to safety. They want to save their money, even when it's compromising their security and privacy."* Despite discouraging their constituents from using public WI-FI, P70 (Türkiye) acknowledged that *"sometimes people may have to use public networks due to financial reasons."* These findings suggest opportunities to make security and privacy solutions more affordable for users in the majority world.

Performance degradation Relatedly, some experts mentioned how following advice can degrade device performance. In particular, some experts indicated that installing anti-virus tools can slow down their resource-constrained devices, as elaborated by P37 (Mexico): *"There are antivirus software on computers that are very slow, well not very slow but they slow down the performance of the computer."* This was echoed by P40 (Brazil) who recalled *"back when I used Windows, I had Norton. Wow, man, for the love of God, that Norton took at least a third of your RAM."* Relatedly, P42 (Brazil) described how VPNs can slow down their connection: *"a VPN makes your connection much slower — five times slower, sometimes. Free VPNs often have limited speeds."*

Not knowing benefits Another reason for not following advice was the fact that some people did not know the security and privacy benefits of following recommended advice. For instance, P44 (Brazil) said that *"it was common for them [people in their community] to say, oh, there's been this update notification for the past five months, and I can't get rid of it."* Similarly, P27 (Ghana) stated that *"most of these updates don't change much. So once they don't see much change after the update, they don't really see the need for updates often."* This was further complicated by the high costs of internet data, as described earlier. Similarly, P36 (Mexico) indicated that people do not use anti-virus because *"they don't know the importance or they simply don't have information about it."* P62 (Pakistan)

emphasized the need to *"reject all besides the necessary cookies . . . So that I've told a lot of people, you know, all your data is going this and that, but you know, a lot of people just like, okay, whatever, we don't care!"*

Social friction due to protective behaviors Social relations and norms in the majority world (highlighted particularly in Ghana and Pakistan) also inhibit people from following advice. For instance, P21 (Ghana) detailed how preventing people from inserting USBs into your devices can cause social friction and negative perceptions, stating that if you *"don't allow people to insert their pendrives to copy music or other kinds of things, they will just say you are being rude and arrogant."* Similarly, P29 (Ghana) described how it can be difficult not to share devices: *"The challenge is normally about our way of doing things. They feel people who need help, if you do not do it [help them], even the reason you give . . . to not share, they feel like you are denying others something."* P64 (Pakistan) narrated how it can be difficult for people in intimate relationships to protect privacy on their devices: *"Sometimes husbands even ask why you've enabled these [security] features. This also leads to issues . . . They themselves say that our family members will question why so many passwords are used."* P62 (Pakistan) added that *"I think since we live in a society where sharing a phone is very common, so . . . if they are sharing their phone a lot, and they have to share, then definitely it's not very feasible to, you know, keep putting in a password yourself every time."* We note that such tensions can dissuade people from taking security and privacy measures such as using a phone lock, and subsequently make them even more vulnerable to IPV via stalkerware.

Language barrier Lastly, some experts described how some of their constituents struggle to use technology devices because they do not understand English. For instance, P54 (India) stated that *"since most of the errors are in English or not even errors, any problem alerts are in English, they do not know what is happening. Say there is some notification on the screen and they did not see what they changed or what they clicked on. For example, there is*

this do-not-disturb service, right? They might have clicked it, accidentally, which eventually leads to their calls being denied. Without them being notified. So stuff like that they don't understand." Similarly, P65 (Pakistan) added that *" if it [the language on tech devices] is in English, they [people they support] don't understand at all."* This language barrier similarly extends to security and privacy, making it difficult for users to understand or configure appropriate privacy controls.

5.3.5.2 Contextual Factors

Overview Lastly, we saw different ways in which factors including gender identity, religion, digital literacy, infrastructural challenges, and device-sharing practices shape security and privacy concerns, advice, and practices in the majority world.

Gender A recent SoK found mixed results regarding the impact of gender on security behaviors in Western contexts [174]. While many quantitative studies find correlations between gender and security and privacy practices, they often fail to account for *why* these correlations exist. Through our study in the majority world, we find a multitude of ways in which gender identity intersects with security and privacy, particularly through perceived threats, barriers to resources and advice, social norms, and gendered seeking of advice. For *perceived threats*, several experts mentioned that women are more vulnerable than men, especially to stalking, image-based sexual abuse, and account compromise. For instance, P27 (Ghana) stated that *"I find a lot of women falling victim to these social media hacks. So you find frequently a lady will call you that someone has hacked my WhatsApp."*

Social norms. Some reasons women are more concerned or vulnerable include cultural expectations to share their devices and patriarchal norms that disadvantage women, similarly noted in majority world countries like Bangladesh [151]. For instance, P10 (Kenya) said that in their rural place, *"women are not given priority when it comes to education and the job accessibility and opportunities and so they have little to no information."*

Gendered seeking of advice. Gender also influences who people turn to for advice. In Pakistan, women prefer to seek advice from other women, as detailed by P60: *"Since I am a girl, more women reach out to me."* In other cases, men experts are preferred for technical challenges, while women are often turned to for sensitive transactions. For instance, P03 (Kenya) said that when people's challenges *"involves some sensitive information, for example . . . their pay slips and all that information, they prefer a female [expert] . . . when it comes to the usual repairs, maybe the usual computers they would prefer a male."* P20 (Nigeria), a woman expert, said that *"even though they [people who seek help] want a male figure [to fix technical problems], I still try to make them understand that I can do this."* However, this does not always work as elaborated by P10 (Kenya): *"The place I am, the way you talk to women is not the way you talk to men . . . When talking to a man, for him to listen to you, another man has to be the one talking to him. [So it's hard to advise men because] they have this diminishing treatment when it comes to women."*

Digital literacy When asked about common challenges in their communities, local experts overwhelmingly pointed to low digital literacy often caused by low literacy. For instance, P02 (Kenya) said that *"most of them [people in their community] are very illiterate and have very little knowledge about ICT."* This low digital literacy often amplifies other challenges, including users forgetting their logins, not understanding privacy controls, and sometimes being vulnerable to stalking. For instance, P08 (Kenya) mentioned how *"the first time someone has created [a] Facebook page or on social media and they end up posting and they might think they have posted for themselves while they have posted and so many other people are seeing it."* P25 (Ghana) described how low digital literacy can make people confuse the camera flashlight on their phones for just a flashlight, and end up unknowingly recording intimate videos of themselves: *"Sometimes the ladies, they give the phones to their children and then in an attempt to use the camera they sometimes walk around nakedly in the room . . . when there is lights out, they use the phone torchlight as a camera even*

if they go to the washroom . . . sometimes in an attempt to put the phone in a good place where they can get the lights they end up punching the video . . . they think they are using the camera light but they do not know that it is the video they have activated." P25 (Ghana) added that *"some people even don't know how to delete things from their phones. When they delete, it go[es] straight to the recycle bin and they have no idea of the recycle bin."* These results show how low digital literacy can amplify security and privacy risks faced by users in the majority world. In fact, prior work in Kenya by Kotut et al. [85] shows that as users (especially non-literate ones) transition from feature phones to smartphones, they encounter issues using these devices, especially if they had memorized feature phone settings, forcing them to rely on other people for help.

Local experts further detailed that they vary their advice and delivery of advice depending on the target users' literacy, and especially digital literacy. For instance, P22 (Ghana) is hesitant to recommend phone locks to people with low digital literacy: *"There are some people who don't know anything at all so if you ask this people to put locks on their phone it will be a problem."* P24 (Ghana) recommends simple passwords for those with low technology skills: *"For those who don't know, I would not make the password very difficult to remember."* Some experts also mentioned not bothering to explain things to people with low literacy levels, instead directly performing the task for them, as elaborated by P58 (Pakistan): *"For uneducated people, we just do this for them. If the person is educated, we will guide him . . . and he will do it himself."* This was echoed by P54 (India): *"If the customer is not educated, then I prefer to solve the problem myself and tell them not to do anything."* Such practices further widen the digital divide between users.

Infrastructural challenges Local experts described various infrastructural challenges that amplify security and privacy challenges and concerns in the majority world. Many experts pointed to poor networks and a lack of access to electricity and personal devices that necessitate their constituents to devise workarounds. For instance, P21 (Ghana) stated

that *"people that do not have access to electricity come here to charge their phones."* If these devices are not adequately protected, e.g., via a PIN, users' information could be accessed at these stations, as confirmed by a recent study in rural Ghana [160]. According to P32 (Mexico), *"the limited access to technology is due to the poverty that prevails in the P'urhépecha area; a good part of the indigenous population does not have a computer, internet or other technological devices at home."* These infrastructural challenges often disproportionately affect rural [160] and indigenous communities, leading to what McClearn et al. refer to as "infrastructuring" [97], i.e., practices such as device sharing and reliance on intermediaries for technology access and use. Due to the security and privacy tensions they introduce, users turn to "patchworking" practices to protect their everyday security [97].

Device-sharing practices Another common theme in our study was device and account sharing. Local experts provided various contexts why they and their constituents share devices and accounts, including at workplaces and at home with trusted ones. P35 (Mexico) explained how device sharing is common in Mexico due to economic constraints: *"Sometimes there is only one device in a single family or worked by a team [adults, young people, and children]. Well, you have to do it on a single computer here. Here, a computer is shared by several people."* P66 (Türkiye) described how sharing is encouraged by their religion: *"If someone in the neighborhood has one [product], that is, if a man who has the means [to] buy it, the neighbors in the neighborhood can borrow it and benefit from it. This is also seen as good from a religious point of view."* However, device sharing can lead people to think they have been "hacked" when their accounts are accessed. In some cases, trust when sharing accounts and devices can be abused, as elaborated by P44 (Brazil): *"The most common issue was with bank passwords. They'd usually share them with other people, like close relatives. Unfortunately, every family has at least one person who's a bit untrustworthy. These people would then make transfers using their name."* We note that these device and account sharing practices routinely lead to privacy tensions.

Religion Religion also influences tech usage and security and privacy concerns in the majority world. Some experts described how religion can turn people away from technology, with P19 (Nigeria) stating that *"Muslims don't have time and they feel most of the things on the Internet are not morally right."* Some experts mentioned being cautious about the advice they give in relation to the advisee's religion. In Türkiye, photo-sharing on social media can be problematic due to religious beliefs as elaborated by P66: *"We had a lot of discussions about . . . whether it is right or permissible to share the picture of your wife, the picture of your daughter or the picture of your son . . . it doesn't matter in the end, if you take and share a picture of your wife, your wife's picture in a home environment that people can't normally see, it zooms in much closer. I mean, it counts your eyebrows, eyes, eyelashes. Is this permissible? It is not . . . It is like this in terms of privacy. In fact, it is also religiously impermissible."* In Pakistan, P59 expressed concern at the Internet blockage during religious holidays: *"My main concern is that the social media platforms should not be blocked at any time. For example, social media gets blocked during Muharram . . . it is harmful not only for our work, but for everyone."*

5.4 Discussion and Conclusion

In this study, we explored security and privacy advice prioritized by local experts (n=70) across nine majority world countries. While local experts' advice for their constituents largely matches advice for their own security and privacy and advice from the West, we surface various significant barriers to advice implementation in the majority world, including economic constraints, language barriers, and social frictions that can be caused by taking protective security and privacy measures.

In this section, we reflect on our findings and share recommendations to better support majority world users. We also share lessons for researchers looking to do similar work.

5.4.1 Main Takeaways

Advice in the majority world is mostly similar to the West Previous research conducted mostly with Western participants finds that the web [128], social media [16, 21, 38, 144, 175], entertainment media [50], and friends and family [51, 65, 67, 110] are common sources of security and privacy advice. We confirm these findings in the majority world. In addition, we find that people in the majority world frequently turn to local experts for advice, with some local experts mentioning they run groups on social media platforms such as WhatsApp and Facebook to disseminate advice. Regarding the advice content, we similarly find that the advice provided (including the use of strong passwords and two-factor authentication) by local experts largely matches advice from the West [71, 128], with advice prioritization challenges [128] similarly extending to the majority world. However, we also noticed some differences. For example, some experts advise their constituents to use memorable passwords likely because their constituents often forget complex passwords. Others advise their constituents to only consult trusted experts. Collectively, these results suggest that recommendations made by previous work in the West around advice prioritization [128] may also be applicable in the majority world. However, without considering the context of the majority world, any such recommendations are likely to fail, and we discuss next why and how advice from the West fails in the majority world.

Western advice fails elsewhere for various reasons While we also find that the trustworthiness of advice [127], convenience [7, 41], past negative incidents [125], and simplicity of advice [125] are critical for implementing advice, we surface factors that make it difficult for users in the majority world to implement advice. For example, our study shows how economic constraints and social frictions that arise because of protective security and privacy practices such as using passwords, inhibit people from following advice. Regular software updates are impractical for some users because of internet costs, while collectivist cultures compel people to share their devices, making it difficult for users to protect their privacy.

Despite advising their constituents to use genuine software, some experts decried how people are unable to afford it, turning to pirated and potentially harmful software. Similarly, other experts mentioned how it is impractical for users to use the often resource-intensive anti-virus tools on their resource-constrained devices. In rural areas, SMS-based two-factor authentication sometimes fails due to poor connectivity. Overall, these results suggest the need for more consideration of users in resource-constrained settings in both the design and deployment of tech and security and privacy solutions.

Many concerns around account "hacking" Throughout our study, one frequently cited concern was account compromise (otherwise described as hacking by many local experts). Local experts recounted various incidents where their own accounts as well as those of other people in their communities had been compromised and taken over. The compromised accounts ranged from social media accounts including Facebook to social messaging apps such as WhatsApp. While the experts described this as hacking, we noted that these "hacks" often involved simple techniques. For instance, several experts detailed how people easily get tricked into giving away one-time authentication codes or clicking on unsuspecting links, resulting in their accounts getting compromised. Device sharing practices can also lead to inadvertent access by users who share the same device. In fact, a recent study focusing on cybercafes in Kenya [103] highlighted how some cybercafe operators encourage their customers to save their passwords in the public computers at the cafes to avoid forgetting them. However, this can result in unauthorized access to user accounts by other cybercafe customers. These concerns point to a need for more educational interventions as well as redesigning technology and security and privacy tools to better serve device sharing practices that remain common in the majority world.

Low literacy amplifies security and privacy risks Our study shows how low digital literacy in the majority world can particularly complicate security and privacy for users. While English is often the de facto language on tech devices and platforms, low-literate users

in the majority world often do not understand English, making it challenging for them to even configure appropriate security and privacy settings. For example, local experts detailed how some users do not understand device update nudges presented in English, turning to the experts to help them to *dismiss* these nudges. Other experts mentioned that some users fail to understand privacy settings and configuration on social networks such as Facebook, leading them to overshare their data. Low literacy also seemed to directly connect with low digital literacy, with experts sharing how low digital literacy makes their constituents vulnerable to risks of being stalked. For example, the ability to log onto multiple WhatsApp accounts on one device can allow attackers to stalk others, especially if the victims do not understand how to check other devices they are logged to. These results suggest opportunities for better language translation for technology and prominent UI features that can provide users with better visibility and transparency into their security and privacy configurations.

5.4.2 Next Steps

Prioritizing advice in the majority world In a previous study focusing on the US, Redmiles et al. [128] noted that there are too many security imperatives on the web, making it difficult for users to prioritize advice. The study recommends the prioritization of a few high-impact pieces of advice for end users. In our study focusing on the majority world, we similarly find a wide variety of security and privacy advice provided by local experts to users. Similar to Redmiles et al., we note that this plethora of advice makes it almost impossible for users to follow all these pieces of advice. Thus, future work can evaluate the efficacy and applicability of security and privacy advice from our work and prior work [125, 127, 128] against the threat models and possible adversaries in the majority world with the goal of prioritizing the most practical and highest impact advice for users in various majority world contexts. For example, in shared device contexts, advice such as logging out of accounts after use might arguably be more useful and practical than the use of strong passwords.

Better translation to local languages Language barrier remains a significant challenge for users in the majority world when using technology, presenting opportunities for better translation from English to local languages. While smartphone brands like Android and Apple allow users to switch languages, these translations are often incomplete, leaving many menus and interfaces in English. Recent advances in AI could be used by tech designers to aid translations to local languages. However, many majority world countries have several local languages, and thus, it's impractical to immediately translate to all these languages. Nevertheless, proper translation to just the official languages would be a good start. Beyond devices, there is also potential to curate security and privacy advice in local languages, ensuring users can better understand and implement important security and privacy advice. As shared by some local experts, public gatherings offer a great avenue to disseminate security and privacy advice. However, adequate care must be taken when doing these translations as security and privacy terms can significantly vary across languages and cultures. Thus, it is crucial to directly work with local communities to account for these nuances during the translation and dissemination of advice.

Designing tech, and security and privacy for diverse contexts Our study underscores the importance for designers to consider diverse contexts in the majority world when designing technology and security and privacy features. For example, password managers could greatly benefit from redesigns that accommodate multiple user profiles, each protected by user-specific vault passwords, to better support device-sharing contexts. This could also be beneficial for experts who manage passwords for other users, e.g., at public computing facilities. Additionally, clearer information about file deletion is needed. While iOS notifies users that deleted items remain in the recycle bin for 30 days, some Android devices do not, leading to misconceptions that deleted files are permanently removed. Nudging users about items in the recycle bin could address this. Similarly, nudges could enhance security in apps like WhatsApp by periodically notifying users of all devices and locations where they are

logged in to alert users about potential stalking. For these designs and interventions to be effective, however, we recommend more research with the target users.

Making tech and security and privacy solutions more affordable In our study, local experts mentioned that pirated software is commonly used by their constituents, despite their advice against using it. To discourage the use of pirated software, companies should make authentic solutions affordable. As economic conditions vary across countries, uniform pricing may be less accessible to users in low-income regions. Instead, we argue that equitable pricing models, such as adjusting for purchasing power parity [131], could improve affordability and encourage the use of genuine and safer software.

5.4.3 Final Thoughts and Future Work

Lessons for the West from the majority world Our results from the majority world show that local experts prioritize usability, affordability, and account access over strictly recommending what may be considered "security best practices" in Western contexts. Even measures they personally adopt, including software updates and the use of VPNs, are not recommended by experts to their constituents if they perceive them to be too costly or complex given the infrastructural and economic realities of their constituents. Local experts additionally emphasize trust and communal approaches to security and privacy, encouraging their constituents to use trusted devices or consult trusted experts only, especially when conducting sensitive transactions. While they have limitations, we believe some of these practices can inform the design of security and privacy solutions that are useful not just in the majority world but also in Western contexts. For instance, making security solutions such as anti-virus less resource-intensive, and genuine software more affordable can also be helpful in Western contexts, especially among low-income groups. Communal approaches to technology access and security and privacy, especially in contexts where trust is essential, are also relevant in settings such as public libraries in the West [37, 91], or between refugees

and their case managers [145]. Thus, designing security and privacy tools suited to these contexts in the majority world will likely be beneficial even in Western contexts.

Future work Our study surfaced how contextual factors — ranging from gender, religion to infrastructural challenges — shape security and privacy concerns and advice. Given that security and privacy practices can be affected by local laws, political regimes, and regulations, future work can explore more closely how these factors shape concerns and advice in the majority world, potentially developing a framework to theorize this relationship.

Chapter 6: Conclusion and Future Work

This dissertation explores the security and privacy challenges and practices of various majority world populations. My investigations begin in Kenya, where I highlight unique security and privacy challenges posed by mobile loan apps and shared public computing facilities at cybercafes. To gain a global perspective, I then explore security and privacy concerns and advice across nine majority world countries. In this chapter, I synthesize key findings from this dissertation and outline promising directions for future research.

6.1 Summary of Key Findings

In this section, I summarize the main findings and contributions of this dissertation.

6.1.1 Impact of Economic Factors on Security and Privacy

A major contribution of this dissertation is demonstrating how financial constraints — which are more pronounced in the majority world — shape users' security and privacy perceptions and practices. In the study on mobile loan apps, I show how financial adversity in Kenya compels many loan apps users to de-prioritize their privacy concerns with these apps in order to secure loans. Similar financial constraints emerged in the cross-national study on security and privacy advice, often acting as a barrier for users implementing advice. For instance, many users cited the cost of internet as a challenge to keeping their devices updated, while others, unable to afford genuine software, resorted to pirated alternatives that may pose security risks. I provide several recommendations that can help address these concerns. For loan apps, simply giving users more transparency and control over their data may be insufficient, as financial need often outweighs privacy considerations. Instead, I advocate for stronger privacy regulations to protect these users. Further, app marketplaces should proactively investigate and take action against apps that misuse user data. After all, there

were numerous privacy complains in the reviews for loan apps on the Google Play Store. I also advocate for more equitable pricing models for tech products and software, particularly based on purchasing power parity [131]; this can make legitimate software affordable and reduce the reliance on pirated and potentially harmful alternatives in the majority world.

6.1.2 Mismatch of Advice Between Western Experts and Local Experts

While there is an overlap between security and privacy advice provided in the West compared to the majority world, this dissertation also highlights notable differences. While Western experts emphasize strong passwords and advise against writing them down, some cybercafe managers in Kenya offer contradicting advice. For instance, some managers encourage customers to use simple passwords such as their names or national ID numbers to remember them. One manager even reuses the same password for all customers. While local experts' advice is adapted to be practical for users in the majority world, it also introduces significant risks to users' account security. My findings suggest the need to collaborate with local experts and communities to understand their practices and threat models to develop security and privacy advice that is both relevant and effective for their communities. For example, I argue that writing down passwords is not problematic as long as users store them securely; this is a much safer approach than using one's name as a password. Further, my work suggests that traditional password-based authentication may not be the most suitable option for these users. Instead, alternatives such as magic links or one-time passwords for each login should be explored, as they may better align with these users' needs and constraints.

6.1.3 Device-Sharing Practices versus Security and Privacy

This dissertation also demonstrates various reasons and contexts for device sharing in the majority world and how these sharing practices complicate security and privacy for users. While prior research in South Asia [136] has shown that women are culturally expected to share their devices, my work extends this to other majority world countries. In particular, I

highlight how financial constraints, social relations, and religious beliefs often compel people to share devices. At the same time, users may feel as though they have been "hacked" when others access their accounts, e.g., because they forgot to log out from shared devices. I argue that security and privacy advice in the majority world should consider these shared-device contexts to be effective and practical for end-users. For instance, users should be advised on the importance of logging out after using shared devices to protect the security and privacy of their accounts. From a technology design perspective, I argue that tools such as password managers should support shared-device contexts. For example, password managers could support multiple user profiles, each protected by user-specific vault passwords, ensuring security while accommodating device sharing practices.

6.1.4 Impact of Socio-Demographic Factors on Security and Privacy

My cross-national study in nine majority world countries further highlights the impact of various socio-demographic factors including gender, religion, socio-economic status, culture among others on security and privacy concerns and practices. For instance, patriarchal norms in some regions continue to marginalize women, restricting their access to essential knowledge and resources, making them more vulnerable online. In countries such as Pakistan, women often prefer seeking help from other women, highlighting the role of gender and social norms in security and privacy practices. Culture also plays a significant role in shaping technology use and security measures. In the majority world, device-sharing remains a common practice, and is sometimes encouraged by religious beliefs. At the same time, this sharing of devices can make it difficult for users to protect their privacy. Overall, these findings emphasize the need to move beyond just technical security and privacy solutions and consider social factors to develop solutions that better protect users' digital safety. It is particularly crucial to explore diverse user groups and collaborate with local communities to design inclusive, culturally-sensitive security and privacy solutions.

6.1.5 Comparison of Findings in the Majority World to Western Contexts

My results and recommendations are different from previous work in Western contexts in several ways. While studies around mobile apps [87] in Western contexts advocate giving users more control and transparency over their data, I argue that this is not sufficient for low socioeconomic users who are willing to overlook their privacy concerns due to competing priorities. Instead, I argue for stakeholders such as regulators and app stores to enforce privacy laws and app store-level measures to protect these users. Comparing practices and concerns at cybercafes in Kenya to public libraries in the US [91], I note some similarities but also differences. First, both library operators and cybercafe managers lack proper training, significantly impacting the advice and support they provide to their customers. However, while library operators in the US are primarily concerned about protecting their clients' privacy from external threats for example governments, cybercafe operators are mostly interested in protecting their customers' security and privacy from other users of the cafes. Further, while the advice provided by most cafe operators appears well-intentioned, security-usability tension often compels them to prioritize account access over security for example by suggesting the use of simple passwords such as names. I recommend the need for more training for the cafe operators as well as a redesign of authentication systems to better serve users in the majority world. Lastly, my cross-national study in the majority world shows how practices such as device-sharing complicate privacy on technology devices. I thus recommend the need to rethink access control in shared device contexts.

6.1.6 Lessons from Conducting Cross-National Research

One contribution of this dissertation are the lessons I share with the security and privacy community on how to appropriately engage with local communities when conducting research. Throughout the process of conducting the cross-national research on security and privacy advice described in chapter 5, the core team and I made deliberate efforts to involve local communities in this work, ranging from recruitment to data collection, analysis, and paper

writing. While this extended the timelines of the project, e.g., because I had to train some local contacts on research, our contacts provided invaluable contributions. They enriched our analysis with a lot of nuances and context that would otherwise have been impossible to capture. We left it up to our contacts to decide their level of involvement, offering various compensation options from payment to authorship and/or both. For payments, we took advantage of platforms including Wise and Remitly to wire payments to our contacts.

For other researchers looking to do similar work, I encourage them to involve local communities to ensure (i) the research benefits directly extend to local communities, and (ii) local context is appropriately respected. While it might be easier and more convenient to use panel providers, I argue that the context and insights provided by local collaborators justify the efforts to involve them. My team and I found it somewhat easier to contact local contacts by tapping into our own academic and personal contacts, an approach that could be beneficial for others looking to replicate our methods. However, we also faced a few challenges. First, this project spanned multiple years because of all the logistics involved in navigating IRB processes, finding the right in-community contacts, handling translations, among others. It was also challenging to coordinate the project across multiple time zones. For others looking to do similar work, I recommend blocking out enough time (in the count of years) and having alternative countries in case others fail to materialize.

6.2 Future Directions

In this section, I now discuss some promising directions for future research to better support users' digital security and privacy in the majority world and beyond.

6.2.1 Exploring Concerns and Advice From the Users' Perspectives

Chapter 5 of this dissertation detailed, for the first time, various security and privacy concerns and advice prioritized by various local experts across nine diverse countries in the majority world. Some of these concerns include fears around account "hacking," misuse of personal

information, financial scams, susceptibility to malware and viruses, and even AI-related concerns such as deepfakes. While the experts mentioned taking as well as advising their constituents to take protective measures including using strong passwords and the use of two-factor authentication, I also found various barriers to implementing these measures including economic constraints, low digital literacy, as well as cultural and social norms that discourage taking protective measures. While these findings provide vital recommendations for how to design security and privacy solutions to support diverse user groups, they are only a starting point, using local experts as a proxy to understand user challenges and practices. Future work should go beyond local experts to interview end-users in the majority world to more directly understand their security and privacy challenges and needs. Such work should particularly explore how common practices such as device-sharing are to inform the design of solutions that can protect users' privacy within these contexts.

6.2.2 Validating Qualitative Findings Through Large-Scale Studies

The qualitative studies and findings presented in this dissertation provide a good initial understanding of the security and privacy challenges faced in several majority world countries. In particular, the qualitative interviews used allowed for a deeper understanding of these challenges, showing for example how economic constraints can make people turn to pirated and potentially harmful software. To explore how these results generalize more broadly to other users, there's opportunities to extend this work through large-scale surveys and measurements. This can be done via analyzing public discourse on social media platforms or through surveys. For instance, a recent study by Akgul et al. [5] analyzed 12 million instances of privacy-related reviews publicly visible on the Google Play Store, finding that the privacy concerns around mobile loan apps detailed in chapter 3 of this dissertation extend far beyond Kenya to other majority world countries such as India. Future work can therefore analyze social media sentiments across countries to see how the concerns and challenges I have detailed in this dissertation extend to other countries. Large-scale surveys could

also help to further explore how these results generalize. Since online survey tools such as Prolific [119] may not be readily available in the majority world, such surveys can use online panel providers that have been used in prior work for example by Herbert et al. [66, 67]

6.2.3 Rethinking Authentication and Password Management

This dissertation qualitatively showed numerous challenges with password management in the majority world. While prior research has explored password selection and challenges in Western contexts [143, 164–166], much less is known about how users in the majority world select and manage their passwords. Further, while tools like password managers have been developed to support users [94, 104, 117], their adoption and suitability in the majority world remain unknown. Future work can examine password selection practices and behaviors in the majority world on a larger scale, as well as user awareness and use of password managers. Additionally, alternative authentication mechanisms, such as magic links and one-time passwords for logins, should be investigated. Understanding and improving password management in the majority world will lead to the design of more usable authentication mechanisms not just for users in the majority world, but for all users more broadly.

6.2.4 Designing Security and Privacy for Shared Contexts

My work suggests that device sharing is a common practice in the majority world, and is driven by economic constraints as well as religious and cultural norms. However, most security and privacy solutions are designed from a Western perspective where device sharing is less common. As a result, these solutions often fail to meet the needs of users in the majority world. Future research can explore how to design security and privacy solutions for shared contexts. For example, password managers could be redesigned to support multiple user profiles, with each profile protected by a vault-specific password known only to its owner. However, it is crucial to involve majority world users in the design and testing process for these tools to ensure they respect and support local contexts.

Bibliography

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

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

[3] CIO Africa. Kenya's E-citizen portal hits 1.23 million. https://cioafrica.co/kenyas-e-citizen-portal-hits-1-23-million/, Feb 2016.

[4] Jenny C. Aker and Isaac M. Mbiti. Mobile Phones and Economic Development in Africa. *Journal of Economic Perspectives*, 24(3):207–32, 2010.

[5] Omer Akgul, Sai Teja Peddinti, Nina Taft, Michelle L Mazurek, Hamza Harkous, Animesh Srivastava, and Benoit Seguin. A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends. In *Proc. USENIX Security*, 2024.

[6] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proc. COMPASS*, 2020.

[7] Elham Al Qahtani, Yousra Javed, Heather Lipford, and Mohamed Shehab. Do Women in Conservative Societies (Not) Follow Smartphone Security Advice? A Case Study of Saudi Arabia and Pakistan. In *Proc. EuroS&PW*, 2020.

[8] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Proc. SOUPS*, 2017.

[9] Iman M. Almomani and Aala Al Khayer. A Comprehensive Analysis of the Android Permissions System. *IEEE Access*, 8:216671–216688, 2020.

[10] Thomas Alsop. Share of households with a computer in Africa 2005-2019. https://www.statista.com/statistics/748549/africa-households-with-computer/#statisticContainer, Nov 2021.

[11] Panagiotis Andriotis, Shancang Li, Theodoros Spyridopoulos, and Gianluca Stringhini. A Comparative Study of Android Users' Privacy Preferences Under the Runtime Permission Model. In *Proc. HAS*, 2017.

[12] Panagiotis Andriotis and Atsuhiro Takasu. To Allow, or Deny? That is the Question. In *Proc. HCI-CPT*, 2020.

[13] Kenya Revenue Authority. https://itax.kra.go.ke/KRA-Portal/, 2022.

[14] Tom L Beauchamp et al. The Belmont Report. *The Oxford textbook of clinical research ethics*, pages 149–155, 2008.

[15] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324, 2004.

[16] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. In *Proc. CSCW*, 2022.

[17] Nicola J. Bidwell. Women and the Sustainability of Rural Community Networks in the Global South. In *Proc. ICTD*, 2020.

[18] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. When the Internet Goes Down in Bangladesh. In *Proc. CSCW*, 2017.

[19] Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. In *Proc. SOUPS*, 2017.

[20] Jasmine Bowers, Imani N. Sherman, Kevin R. B. Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proc. WiSec*, 2019.

[21] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proc. CHI*, 2021.

[22] Rex Bringula, Jenmart Bonifacio, Ana Natanauan, Mikael Manuel, and Katrina Panganiban. Pattern of internet usage in cyber cafés in Manila: An exploratory study. *International Journal of Cyber Society and Education*, 5(2):152–164, 2012.

[23] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proc. SOUPS*, 2019.

[24] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. In *Proc. IEEE S&P*, 2018.

[25] Africa Check. What share of households in Kenya own a computer? https://africacheck.org/infofinder/explore-facts/what-share-households-kenya-own-computer, May 2020.

[26] Pern Hui Chia, Yusuke Yamamoto, and N. Asokan. Is This App Safe? A Large Scale Study on Application Permissions and Risk Signals. In *Proc. WWW*, 2012.

[27] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009.

[28] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project, Jul 2006. http://www.qualres.org/.

[29] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Reem Talhouk. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proc. CHI*, 2018.

[30] Kovila PL Coopamootoo and Magdalene Ng. "Un-Equal Online Safety?" A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns. In *Proc. USENIX Security*, 2023.

[31] Sadie Creese, William H Dutton, and Patricia Esteve-González. The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and ubiquitous computing*, 25(5):941–955, 2021.

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

[33] CyberCafePro. CyberCafePro is Cyber Cafe Management Software. https://cybercafepro.com/, 2022.

[34] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G. Bardas. Defensive Technology Use by Political Activists During the Sudanese Revolution. In *Proc. IEEE S&P*, 2021.

[35] Martynas Damulis. Investigations of Financial Fraud: Literature Analysis of Selected Financial Scams. *Theory and Practice of Illegitimate Finance*, pages 203–221, 2023.

[36] DataReportal. Digital 2023: Pakistan. https://datareportal.com/reports/digital-2023-pakistan, 2023.

[37] Samuel Dooley, Michael Rosenberg, Elliott Sloate, Sungbok Shin, and Michelle Mazurek. Libraries' Approaches to the Security of Public Computers. In *Proc. WIPS*, 2020.

[38] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholson, John McCarthy, and Patrick Olivier. Social Media As a Resource for Understanding Security Experiences: A Qualitative Analysis of #Password Tweets. In *Proc. SOUPS*, 2015.

[39] eCitizen. A portal that offers access to information and services provided by the Kenyan government. https://www.ecitizen.go.ke/ecitizen-services.html, 2015.

[40] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Towards Detecting Compromised Accounts on Social Networks. *IEEE Transactions on Dependable and Secure Computing*, 14(4):447–460, 2015.

[41] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Proc. SOUPS*, 2016.

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

[43] Mark Felsenthal and Ryan Hahn. Financial inclusion on the rise, but gaps remain, Global Findex database shows, Apr 2018.

[44] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android Permissions Demystified. In *Proc. CCS*, 2011.

[45] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Proc. SOUPS*, 2012.

[46] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[47] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proc. CHI*, 2018.

[48] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.*, 1(CSCW), 2017.

[49] Freedom House. Freedom on the net: Scores by country. https://freedomhouse.org/countries/freedom-net/scores, 2024.

[50] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The Effect of Entertainment Media on Mental Models of Computer Security. In *Proc. SOUPS*, 2019.

[51] Susanne Furman, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton. Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy*, 10(2):40–49, 2011.

[52] Benjamin Gardner. Incentivised snowballing. *The Psychologist*, 22(9):768–769, 2009.

[53] Samuel Gitta and J Robert Ikoja-Odongo. The impact of cybercafés on information services in Uganda. *First Monday*, 2003.

[54] Ricardo Gomez and Luis Fernando Baron-Porras. Does public access computing really contribute to community development? Lessons from libraries, telecentres and cybercafés in Colombia. *The Electronic Journal of Information Systems in Developing Countries*, 49(1):1–11, 2011.

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

[56] Julie M. Haney and Wayne G. Lutters. It's Scary... It's Confusing... It's Dull: How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proc. SOUPS*, 2018.

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

[58] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proc. SOUPS*, 2014.

[59] Eszter Hargittai. Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4), 2002.

[60] Eszter Hargittai. The Digital Divide and What To Do About It. *New economy handbook*, 2003:821–839, 2003.

[61] Ayako A Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. How WEIRD is Usable Privacy and Security Research? In *Proc. USENIX Security*, 2024.

[62] Anikar Michael Haseloff. Cybercafés and their potential as community development tools in India. *The Journal of Community Informatics*, 1(3), 2005.

[63] Sumair Ijaz Hashmi, Rimsha Sarfaraz, Lea Gröber, Mobin Javed, and Katharina Krombholz. Understanding the Security Advice Mechanisms of Low Socioeconomic Pakistanis. In *Proc. CHI*, 2025.

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

[65] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. Digital Security—A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups. In *Proc. IEEE S&P*, 2024.

[66] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A World Full of Privacy and Security (Mis)Conceptions? Findings of a Representative Survey in 12 Countries. In *Proc. CHI*, 2023.

[67] Franziska Herbert, Collins W Munyendo, Jonas Hielscher, Steffen Becker, and Yixin Zou. Digital Security Perceptions and Practices Around the World: A WEIRD versus Non-WEIRD Comparison. In *Proc. USENIX Security*, 2025.

[68] Jay Hoffmann. The window at the cafe. https://thehistoryoftheweb.com/the-window-at-the-cafe/, Jul 2017.

[69] Abdellah Houmz, Mohamed Salim Mezzene, Asmaa Tellabt, Ghita Mezzour, and Mohammed El Koutbi. Field study of cybercafé usage & security in Morocco. In *Proc. IEEE ACOSIS*, 2016.

[70] Faheem Hussain, Abdullah Hasan Safir, Dina Sabie, Zulkarin Jahangir, and Syed Ishtiaque Ahmed. Infrastructuring Hope: Solidarity, Leadership, Negotiation, and ICT among the Rohingya Refugees in Bangladesh. In *Proc. ICTD*, 2020.

[71] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proc. SOUPS*, 2015.

[72] Aarti Israni, Nicole B Ellison, and Tawanna R Dillahunt. 'a library of people' online resource-seeking in low-income communities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–28, 2021.

[73] Margaret C. Jack, Pang Sovannaroth, and Nicola Dell. "Privacy is Not a Concept, but a Way of Dealing with Life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), 2019.

[74] William Jack and Tavneet Suri. Mobile money: The economics of M-PESA. Technical report, National Bureau of Economic Research, 2011.

[75] Alex Johnson. Equifax breaks down just how bad last year's data breach was. https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496, 2018.

[76] Ryan Johnson, Zhaohui Wang, Corey Gagnon, and Angelos Stavrou. Analysis of Android Applications' Permissions. In *Proc. SERE-C*, 2012.

[77] Anne Jonas, Stefani Vargas, and Jean Hardy. 'Better than Google': Information Activism for LGBTQ+ Young Adults in a Rural Community. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW2), November 2024.

[78] G. Karjoth and M. Schunter. A privacy policy model for enterprises. In *Proc. CSFW*, 2002.

[79] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Proc. FC*, 2012.

[80] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as Part of the App Decision-Making Process. In *Proc. CHI*, 2013.

[81] A. Khatoon and P. Corcoran. Android permission system and user privacy — A review of concept and approaches. In *Proc. ICCE*, 2017.

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

[83] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in Germany through qualitative interviews. In *Proc. USENIX Security*, 2024.

[84] Lindah Kotut. Terms and Conditions (Do Not) Apply: Understanding Exploitation Disparities in Design of Mobile-Based Financial Services. In *Proc. AfriCHI*, 2025.

[85] Lindah Kotut and Hummd Alikhan. "Things on the Ground are Different"': Utility, Survival and Ethics in Multi-Device Ownership and Smartphone Sharing Contexts. In *Proc. CHI*, 2024.

[86] Neha Kumar, Waylon Brunette, Nicola Dell, Trevor Perrier, Beth Kolko, Gaetano Borriello, and Richard Anderson. Understanding Sociotechnical Implications of Mobile Health Deployments in India, Kenya, and Zimbabwe. *Information Technologies & International Development*, 11(4):pp–17, 2015.

[87] Ilaria Liccardi, Joseph Pato, and Daniel J Weitzner. Improving mobile app selection through transparency and better permission analysis. *Journal of Privacy and Confidentiality*, 5(2):1–55, 2014.

[88] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *Proc. SOUPS*, 2014.

[89] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. How WEIRD is CHI? In *Proc. CHI*, 2021.

[90] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proc. SOUPS*, 2016.

[91] Alan F. Luo, Noel Warford, Samuel Dooley, Rachel Greenstadt, Michelle L. Mazurek, and Nora McDonald. How Library IT Staff Navigate Privacy and Security Challenges and Responsibilities. In *Proc. USENIX Security*, 2023.

[92] Moses Muia Masika, Gregory Barnabas Omondi, Dennis Simiyu Natembeya, Ephraim Mwatha Mugane, Kefa Ogonyo Bosire, and Isaac Ongubo Kibwage. Use of mobile learning technology among final year medical students in Kenya. *Pan African Medical Journal*, 21(1), 2015.

[93] MAXQDA. https://www.maxqda.com/, 2024.

[94] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why users (don't) use password managers at a large educational institution. In *Proc. USENIX Security*, 2022.

[95] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. "Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *Proc. USENIX Security*, 2021.

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

[97] Jessica Mcclearn, Rikke Bjerg Jensen, and Reem Talhouk. Security Patchworking in Lebanon: Infrastructuring Across Failing Infrastructures. *Proc. ACM on Human-Computer Interaction*, 8(CSCW1), 2024.

[98] Nora McDonald, Rachel Greenstadt, and Andrea Forte. Intersectional Thinking about PETs: A Study of Library Privacy. In *Proc. PETS*, 2023.

[99] 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), 2019.

[100] Mohammad Basir Moqemi. The Interplay Between Social Harm and Education: Toward Preventing Societal Detriment. *Sprin Journal of Arts, Humanities and Social Sciences*, 2(12):82–90, 2023.

[101] Deepthi Mungara, Harshini Sri Ramulu, and Yasemin Acar. Security and Privacy Advice for UPI Users in India. In *Proc. USENIX Security*, 2025.

[102] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. In *Proc. IEEE S&P*, 2022.

[103] Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv. "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *Proc. IEEE S&P*, 2023.

[104] Collins W Munyendo, Peter Mayer, and Adam J Aviv. "I just stopped using one and started using the other"': Motivations, Techniques, and Challenges When Switching Password Managers. In *Proc. CCS*, 2023.

[105] Collins W Munyendo, Kentrell Owens, Faith Strong, Shaoqi Wang, Adam J Aviv, Tadayoshi Kohno, and Franziska Roesner. "You Have to Ignore the Dangers"': User Perceptions of the Security and Privacy Benefits of WhatsApp Mods. In *Proc. IEEE S&P*, 2024.

[106] Collins W. Munyendo, Veronica A. Rivera, Jackie Hu, Emmanuel Tweneboah, Amna Shahnawaz, Karen Sowon, Dilara Keküllüoğlu, Marcos Silva, Yue Deng, Mercy Omeiza, Gayatri Priyadarsini Kancherla, Maria Rosario Niniz Silva, Maryam Mustafa, Abhishek Bichhawat, Francisco Marmolejo-Cossio, Elissa M. Redmiles, and Yixin Zou. "I Wonder if These Warnings Are Accurate": Security and Privacy Advice in Nine Majority World Countries. In *Proc. IEEE S&P*, 2026.

[107] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. In *Proc. CHI*, 2021.

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

[109] NACOSTI. National Commission for Science, Technology and Innovation. https://www.nacosti.go.ke/, Oct 2022.

[110] James Nicholson, Lynne Coventry, and Pamela Briggs. "If It's Important It Will Be A Headline"': Cybersecurity Information Seeking in Older Adults. In *Proc. CHI*, 2019.

[111] Anri Nishnianidze. Surveillance in the Digital Age. *ESI Preprints*, 24:80–80, 2023.

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

[113] Nathan Oyori Ogechi. On language rights in Kenya. *Nordic Journal of African Studies*, 12(3):19–19, 2003.

[114] Anna-Marie Ortloff, Jenny Tang, Arthi Arumugam, Daniel Huschina, Lisa Geierhaas, Florin Martius, Luisa Jansen, Kolja von der Twer, Lilly Jungbluth, and Matthew Smith. Replication: "no one can hack my mind"' - 10 years later: An update and outlook on experts' and non-experts' security practices and advice. In *Proc. SOUPS*, 2025.

[115] Cliodhna O'Connor and Helene Joffe. Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, 19, 2020.

[116] Aswati Panicker, Novia Nurain, Zaidat Ibrahim, Chun-Han Wang, Seung Wan Ha, Yuxing Wu, Kay Connelly, Katie A Siek, and Chia-Fang Chung. Understanding fraudulence in online qualitative studies: From the researcher's perspective. In *Proc. CHI*, 2024.

[117] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Proc. SOUPS*, 2019.

[118] Jacob Poushter. Smartphone ownership and internet usage continues to climb in emerging economies. *Pew Research Center*, 22(1):1–44, 2016.

[119] Prolific. https://www.prolific.com/, 2024.

[120] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M Redmiles. "Did They F*** ing Consent to That?": Safer Digital Intimacy via Proactive Protection Against Image-Based Sexual Abuse. In *Proc. USENIX Security*, 2024.

[121] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proc. SOUPS*, 2012.

[122] Divya Ramesh, Vaishnav Kameswaran, Ding Wang, and Nithya Sambasivan. How Platform-User Power Relations Shape Algorithmic Accountability: A Case Study of Instant Loan Platforms and Financially Stressed Users in India. In *Proc. FACCT*, 2022.

[123] Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proc. USENIX Security*, 2015.

[124] Elissa M Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *Proc. IEEE S&P*, 2019.

[125] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proc. CCS*, 2016.

[126] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proc. CHI*, 2017.

[127] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Proc. IEEE S&P*, 2016.

[128] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proc. USENIX Security*, 2020.

[129] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[130] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'I have too much respect for my elders': Understanding South African Mobile Users' Perceptions of Privacy and Current Behaviors on Facebook and WhatsApp. In *Proc. USENIX Security*, 2020.

[131] World Population Review. Purchasing Power Parity by Country 2024. https://worldpopulationreview.com/country-rankings/purchasing-power-parity-by-country, 2024.

[132] Kathryn Roulston. *Analysing interviews*. The SAGE handbook of qualitative data analysis, 2014.

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

[134] Dina Sabie and Syed Ishtiaque Ahmed. Moving into a technology land: exploring the challenges for the refugees in Canada in accessing its computerized infrastructures. In *Proc. COMPASS*, 2019.

[135] Kavous Salehzadeh Niksirat, Collins W Munyendo, Onicio Batista Leal Neto, Muswagha Katya, Cyrille Kouassi, Kevin Ochieng, Angoa Georgina, Bernard Olayo, Jean-Philippe Barras, Ciro Cattuto, et al. Reimagining Wearable-Based Digital Contact Tracing: Insights from Kenya and Côte d'Ivoire. In *Proc. CHI*, 2025.

[136] 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. In *Proc. SOUPS*, 2018.

[137] Nithya Sambasivan, Ed Cutrell, Kentaro Toyama, and Bonnie Nardi. Intermediated technology use in developing communities. In *Proc. CHI*, 2010.

[138] Benjamin Saunders, Jenny Kitzinger, and Celia Kitzinger. Anonymising interview data: challenges and compromise in practice. *Qualitative Research*, 15(5):616–632, 2015.

[139] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proc. CHI*, 2017.

[140] Juliane Schmüser, Harshini Sri Ramulu, Noah Wöhler, Christian Stransky, Felix Bensmann, Dimitar Dimitrov, Sebastian Schellhammer, Dominik Wermke, Stefan Dietze, Yasemin Acar, and Sascha Fahl. Analyzing Security and Privacy Advice During the 2022 Russian Invasion of Ukraine on Twitter. In *Proc. CHI*, 2024.

[141] Sarita Schoenebeck, Amna Batool, Giang Do, Sylvia Darling, Gabriel Grill, Daricia Wilkinson, Mehtab Khan, Kentaro Toyama, and Louise Ashwell. Online Harassment in Majority Contexts: Examining Harms and Remedies across Countries. In *Proc. CHI*, 2023.

[142] Tanusree Sharma, Md Mirajul Islam, Anupam Das, SM Taiabul Haque, and Syed Ishtiaque Ahmed. Privacy during pandemic: A global view of privacy practices around covid-19 apps. In *Proc. COMPASS*, 2021.

[143] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Can Long Passwords Be Secure and Usable? In *Proc. CHI*, 2014.

[144] Lucy Simko, Adryana Hutchinson, Alvin Isaac, Evan Fries, Micah Sherr, and Adam J. Aviv. "Modern problems require modern solutions"': Community-Developed Techniques for Online Exam Proctoring Evasion. In *Proc. CCS*, 2024.

[145] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *Proc. IEEE S&P*, 2018.

[146] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. In *Proc. CHI*, 2019.

[147] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They Look at Vulnerability and Use That to Abuse You"': Participatory Threat Modelling with Migrant Domestic Workers. In *Proc. USENIX Security*, 2022.

[148] Karen Sowon, Collins W Munyendo, Lily Klucinec, Eunice Maingi, Gerald Suleh, Lorrie Faith Cranor, Giulia Fanti, Conrad Tucker, and Assane Gueye. Design and Evaluation of Privacy-Preserving Protocols for Agent-Facilitated Mobile Money Services in Kenya. In *Proc. SOUPS 2025*, 2025.

[149] Laura D Stanley. Beyond access: Psychosocial barriers to computer literacy. *The Information Society*, 19(5):407–416, 2003.

[150] Statista. Smartphone penetration worldwide by country. https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/, 2022.

[151] Sharifa Sultana, François Guimbretière, Phoebe Sengers, and Nicola Dell. Design Within a Patriarchal Society: Opportunities and Challenges in Designing for Rural Women in Bangladesh. In *Proc. CHI*, 2018.

[152] Sharifa Sultana, Ilan Mandel, Shaid Hasan, S.M.Raihanul Alam, Khandaker Reaz Mahmud, Zinnat Sultana, and Syed Ishtiaque Ahmed. Opaque Obstacles: The Role of Stigma, Rumor, and Superstition in Limiting Women's Access to Computing in Rural Bangladesh. In *Proc. COMPASS*, 2021.

[153] Rabia Tahir. A Study on Malware and Malware Detection Techniques. *International Journal of Education and Management Engineering*, 8(2):20, 2018.

[154] Techopedia. What is a Cybercafe? - definition from Techopedia. https://www.techopedia.com/definition/6701/cybercafe, Apr 2016.

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

[156] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences. In *Proc. SOUPS*, 2017.

[157] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *Proc. USENIX Security*, 2020.

[158] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proc. CHI*, 2022.

[159] Lilian Tuwei, W Sakataka, and E Oteki. Credit reference bureau as the factor influencing the profitability of commercial banks in Kenya: A case of Standard Chartered Bank, Kenya. *International Journal of Novel Research in Marketing Management and Economics*, 2(3):122–129, 2015.

[160] Emmanuel Tweneboah, Collins W Munyendo, and Yixin Zou. "No, I Can't Be a Security Personnel on Your Phone"': Security and Privacy Threats From Sharing Infrastructure in Rural Ghana. In *Proc. USENIX Security*, 2025.

[161] Rebecca Umbach, Anubha Singh, and Ashley Walker. "Your Protection is in Your Hands Only"': User Awareness and Adoption of Privacy and Security Practices in Five Majority World Countries. *Journal of Online Trust and Safety*, 2(1), 2023.

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

[163] United Nations Development Programme. Gender inequality index (gii). https://hdr.undp.org/data-center/thematic-composite-indices/gender-inequality-index/indicies/GII, 2024.

[164] Blase Ur. *Supporting Password-Security Decisions with Data.* PhD thesis, Carnegie Mellon University, USA, 2016.

[165] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proc. CHI*, 2016.

[166] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Proc. SOUPS*, 2015.

[167] Jan Van Dijk and Kenneth Hacker. The digital divide as a complex and dynamic phenomenon. *The information society*, 19(4):315–326, 2003.

[168] Courtland VanDam, Jiliang Tang, and Pang-Ning Tan. Understanding Compromised Accounts on Twitter. In *Proc. WI*, 2017.

[169] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining Security and Privacy Research in Developing Regions. In *Proc. COMPASS*, 2018.

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

[171] Victim Support. Image-based sexual abuse. https://www.victimsupport.org.uk/crime-info/types-crime/image-based-sexual-abuse/, 2025.

[172] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. "I Knew It Was Too Good to Be True"' The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–25, 2018.

[173] Zuoguang Wang, Limin Sun, and Hongsong Zhu. Defining Social Engineering in Cybersecurity. *IEEE Access*, 8:85094–85115, 2020.

[174] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M Redmiles, and Franziska Roesner. SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. In *Proc. USENIX Security*, 2024.

[175] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Proc. SOUPS*, 2022.

[176] Nicola Wendt, Rikke Bjerg Jensen, and Lizzie Coles-Kemp. Civic Empowerment through Digitalisation: The Case of Greenlandic Women. In *Proc. CHI*, 2020.

[177] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. Android Permissions Remystified: A Field Study on Contextual Integrity. In *Proc. USENIX Security*, 2015.

[178] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In *Proc. IEEE S&P*, 2017.

[179] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. Contextualizing Privacy Decisions for Better Prediction (and Protection). In *Proc. CHI*, 2018.

[180] World Bank. Individuals using the internet (% of population). https://data.worldbank.org/indicator/IT.NET.USER.ZS, 2024.

[181] Worldometer. Population by country (2024). https://www.worldometers.info/world-population/population-by-country, 2024.

[182] Worldometer. GDP by Country. https://www.worldometers.info/gdp/gdp-by-country/, 2025.

[183] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. What Makes a "Bad"' Ad? User Perceptions of Problematic Online Advertising. In *Proc. CHI*, 2021.

[184] Eric Zeng, Xiaoyuan Wu, Emily N Ertmann, Lily Huang, Danielle F Johnson, Anusha T Mehendale, Brandon T Tang, Karolina Zhukoff, Michael Adjei-Poku, Lujo Bauer, et al. Measuring Risks to Users' Health Privacy Posed by Third-Party Web Tracking and Targeted Advertising. In *Proc. CHI*, 2025.

[185] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *Proc. USENIX Security*, 2021.

[186] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. "I've Got Nothing to Lose"': Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Proc. SOUPS*, 2018.

Appendix A: Mobile Loan Apps

A.1 Interview Script

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

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

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

2. What mobile loan app have you most commonly used?
3. Please describe how this application works.
   Ask below follow-up questions if they are not addressed.
   (a) How does it calculate your credit worthiness?
   (b) What happens if you're unable to pay back the loan?
4. Why do you use this mobile loan application?
5. What do you like the most about this mobile loan app?
6. What do you dislike the most about this mobile loan app?
7. Do you have any concerns with this mobile loan app?
   Ask below follow-up question if it is not mentioned.
   (a) Any security and privacy concerns?
8. Have you stopped using any mobile loan application?
   Ask below follow-up questions if they are not addressed.
   (a) What loan application?
   (b) Why did you stop using it?
9. Have you removed any mobile loan app after using it?
   Ask below follow-up questions if they are not addressed.
   (a) What loan application?
   (b) Why did you remove it?
10. All mobile applications require access to different permissions in order to access data required for one function or another. Mobile loan applications similarly require access to different permissions. What are the permissions required by the mobile loan application you have most commonly used or use?
    Guide participants through the process if they are unfamiliar with it.
    (a) What do you think this loan application does with these permissions?
    Ensure participants provide an answer for all the permissions.
    (b) How did you learn about this?
    (c) Are you comfortable with this?

11. What permissions requested by mobile loan apps, if any, are you least concerned about?
12. What permissions requested by mobile loan apps, if any, are you most concerned about?
13. Is there anything else you would like to share about mobile loan apps?
14. As a result of this interview, is there anything you will do differently with mobile loan applications going forward?

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

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

A.2 Codebook

- **mobile-loan-apps (64)**
  Tala (14), Branch (13), OKash (8), OPesa (5), Zenka (5), Zash (2), LCash (2), MoKash (2), iCash (2), Timiza (2), iPesa (2), MyKES (1), Scoppe (1), Berry (1), CashNow (1), CreditHela (1), LionCash (1), CashApp (1)
- **loan-app-permissions (129)**
  contacts (20), SMS (20), telephone (20), location (19), storage(19), camera (16), calendar (10), microphone (5)
- **permissions-use (140)**
  SMS (26): *check-transactions (10), send-you-SMS-reminders (5), know-frequent-contacts (4), check-loan-defaults (2), phone-verification (2), text-contacts (1), send-you-updates (1), send-you-promotional-texts (1)*

  contacts (22): *call/SMS-them-upon-defaulting (17), access/confirm-guarantors (3), call-you (2)*

  location (22): *track-you (14), confirm-location (5), don't-know (2), customize-services (1)*

  telephone (19): *don't-know (5), reminder-calls (3), send-you-money (3), track-you (2), confirm-phone-ownership (2), promotional-calls (1), call-contacts (1), check-phone-type (1), check-frequent-contacts (1)*

  camera (18): *don't-know (7), take/upload-photo (6), assess-you/looks (3), track-you (1), spy-on-you (1)*

  storage (18): *don't-know (12), app-installation (3), access-files (1), install-backdoor (1), check-other-apps (1)*

  calendar (10): *know-pay-day (5), record-keeping (2), know-borrowing-date (1), locate-you (1), don't-know (1)*

  microphone (5): *don't-know (2), talk-to-agent (2), record-you (1)*

- **loan-app-positives (38)**
  quick-loan-disbursement (14), growing-borrowing-limits (7), no-paperwork/formalities-required (6), easy-access-to-loans (3), promotions/offers (2), small-interest-rates (2), MPesa-intergration (1), apps-have-reminders-to-pay (1), apps-don't-need-lending-reason (1), adequate-loan-amounts (1)
- **credit-worth-calculation (24)**
  trust (5), check-transactions (4), don't-know (4), employment-details (4), check-CRB (3), data-from-permissions (2), social-media-data (1), telecoms-company-data (1)
- **loan-app-concerns (67)**
  frequent-calls/SMS (13), borrowing-addiction (13), high-interest-rate (10), short-repayment-period (6), growing-interest (6), CRB-listing (4), data-shared-with-third-parties (4), penalties-for-delayed-payment (3), interest-deducted-upfront (2), no-option-to-delete-info (1), don't-know-data-handling (1), app-records-passwords (1), social-media-shaming (1), small-loan-amounts (1), other-people-borrowing (1)
- **concerning-permissions (35)**
  contacts (24): *contacts-not-involved-in-loan (9), contacts-will-be-threatened (5), name-defamation (5), apps-should-stick-to-guarantors (4), contacts-will-be-tracked (1)*

  camera (5): *spy-on-you (3), don't-know-use (2)*

  SMS (2): *read-private-messages (2)*

  location (2): *track-you (2)*

  storage (2): *don't-know-use (1), app-will-misuse (1)*
- **non-concerning-permissions (26)**
  storage (6): *don't-know-use (5), required-for-app-installation (1)*

  location (6): *can-easily-move (3), required/already-provided (3)*

  camera (4): *don't-know-use (2), take/upload-photo (1), immediately-remove-app-after-use (1)*

  telephone (3): *don't-know-use (2), app-already-has-access (1)*

  calendar (2): *don't-know-use (2), calendar-empty (1)*

  contacts (2): *verify-guarantor (1), publicly-available (1)*

  SMS (2): *no-private-SMS (1), comfortable-receiving-texts-from-app (1)*
- **loan-privacy-tradeoff (10)**
  disregard-privacy-to-get-loan (10)
- **post-interview-behaviour (10)**
  avoid/won't-use-loan-apps (6), check-permissions-before-use (3), minimize-usage (1)
- **additional-information (4)**
  regulate-loan-apps (4)

Appendix B: Cybercafes

B.1 Interview Script

B.1.1 Interview Script - Cybercafe Managers

General Questions

1. Can you please explain to me whether you own this cybercafe?
   (a) Yes: Why did you establish it?
   (b) No: Why did you choose to work here?
2. How long have you operated, worked at, or owned this cybercafe?
3. Please describe the equipment or computers in the cybercafe.
   (a) How many computers? How many printers? What software?
   (b) How frequently is the software updated? Why or why not?
4. Do you provide any other services other than cybercafe services?
5. How many customers do you have in a typical week?
6. What are the characteristics of your customers?
   (a) Dominant age group? Gender? Socio-economic background?
7. Can you please share some of the challenges you have faced operating this cybercafe, if there are any?

Cybercafe Services

8. Based on your observations, what websites or services do your customers most typically use or visit at your cybercafe?
9. Are there services that customers ask for that you cannot provide? Please explain why you do or do not provide that service.
10. How often do you have first-time customers at your cybercafe?
    (a) What services are these customers usually seeking?

User Challenges

11. When a customer has a technical challenge, what are some of these challenges? Can you provide any examples?
    (a) Examples might include setting up an account or even actual tasks. Please elaborate.
12. To follow up, do these customers ask you for advice or help?
    (a) What kind of advice or help do you provide?
    (b) Are the issues resolved after you help? If not, why not?

General Advice

13. When you are asked for advice, what information or expertise do you rely on to help?
    (a) Examples include your personal experience. Please elaborate.
14. Do you vary your advice or guidance for the customers?

(a) How might advice differ from an inexperienced customer compared to a more experienced customer?

(b) Do you have examples of this occurring? Please elaborate.

15. When you provide advice or guidance, do the customers follow it? Why or why not?

16. Has there ever been a situation where you were asked for help or advice where you did not know the right answer?

    (a) If so, what was the question? And what answer did you provide?

    (b) If not, what was the most challenging question received and what help did you provide?

Security and Privacy Advice

I am now going to ask you general questions about security and privacy. There are no wrong answers, I am simply interested in your thoughts.

17. In your opinion, what are the top three things you can do or someone else can do to stay safe online?

    (a) For each, ask them to elaborate.

    (b) For each, ask them if they follow this advice.

    (c) For each, ask them if they have offered this advice to any customers, and elaborate on that situation.

    (d) For each, what would happen if you don't follow this advice.

18. What is your greatest concern online with respect to your personal security or privacy? Follow up with elaboration.

Users' Security and Privacy

19. Are there any standard practices at the cybercafe regarding the security and privacy of your customers?

    (a) If not, explain more about what you do.

    (b) If so, [for each] provide some detail on that policy and practice and why you do it.

20. Do you have any concerns regarding how customers might use the computers? Please elaborate.

    (a) Yes: Do you take any precautions to prevent those actions?

    (b) No: Why are you not concerned?

21. Do you have any general security practices for updating and maintaining the computers? Please elaborate.

22. Is there anything you do after a user has finished using a computer?

    (a) Do you reset the session? Why or why not.

    (b) Do you log them out, or ask them to log out? Why or why not.

Miscellaneous

23. Is there anything else you would like to share about your experience owning or operating this cybercafe?

24. I am also planning to speak to cybercafe customers about their experiences. Is there anything I should know or advice you can provide for those conversations?

Demographics

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

25. Do you own a smartphone?

(a) Is it a work or personal phone? What is the phone type and model?

26. Do you own a computer or laptop?

    (a) Yes: Is it a personal or work computer?

27. What is your age?

28. What is your gender?

29. What is the highest level of education you have attained?

30. Do you have a background in IT or computers as part of your work experience or school beyond working or owning the cybercafe?

31. Do you have any feedback or questions about this interview?

B.1.2 Interview Script - Cybercafe Customers

General Questions

1. Please tell me a little bit about yourself and what you do.

2. Why do use cybercafes?

    (a) What is a typical thing you do at the cybercafe? Why do you do this at the cybercafe rather elsewhere?

3. What do you like the most about cybercafes and why?

4. What do you dislike the most about cybercafes and why?

Cybercafe Usage

5. How often do you use or go to cybercafes?

    (a) In a month? In a week? In a day?

    (b) First time users: Do you see yourself coming to the cybercafe again? How often?

6. How much time (in hours) do you typically spend at the cybercafe when you go there?

    (a) Can you provide an example of a task that takes more time than others when you come to the cybercafe?

7. What do you normally consider when choosing a cybercafe to go to?

    (a) Examples include the location of the cyber etc.

User Challenges

8. Are there any technical challenges you have faced when using cybercafes? Examples include using the computer or printing a document.
   If user has faced a challenge...

    (a) How did you (or do you) resolve these challenges?

    (b) Did you ask for help? From whom and why?

    (c) What help or advice was provided?

    (d) Did you follow this advice/help? Why or why not?

    (e) Are you satisfied with the help you received? Why or why not?

        i. If not, is there anything else you did to reach satisfaction?

If user has not faced any challenge...

(a) Why do you think you have not faced any challenges?

(b) Are the tasks you do there easy or difficult? Please elaborate.

9. Have you received any assistance or guidance relating to security and privacy? Examples include selecting your password. Please elaborate.
If the user has received assistance...

(a) What advice or guidance was provided?

(b) Who provided this advice?

(c) Did you or do you follow the advice? Why or why not?

(d) Has this advice influenced your behavior online? e.g how you create other passwords?

If the user has not received any assistance...

(a) Do you have any sources of advice or guidance relating to security and privacy for example how you select your passwords?

i. Examples include friends etc. Please elaborate.

(b) How did you learn about these sources?

(c) Why do you follow the advice?

(d) Has this advice influenced your behavior online e.g how you create other passwords?

10. Take me through what you do on websites or your accounts when you're done using the cybercafe.

(a) Do you sign out of your accounts? Why or why not?

Security and Privacy Advice
I am now going to ask you general questions about security and privacy. There are no wrong answers, I am simply interested in your thoughts.

11. In your opinion, what are the top three things you can do or someone else can do to stay safe online?

(a) For each, ask them to elaborate.

(b) For each, ask them if they follow this advice.

(c) For each, what would happen if you don't follow this advice.

12. What is your greatest concern online with respect to your personal security or privacy? Follow up with elaboration.

Device Questions

13. What type of phone do you use? (Is it a feature or a smartphone?)

(a) If smartphone: Do you access the internet on your device? What are some of the websites or services you use?

14. Do you share your phone with others?

(a) Yes: With whom and why?

(b) No: Why not?

15. Do you have any concerns with access to your phone?

(a) Concerned: What concerns? What do you do to prevent this?

(a) Not concerned: Why are you not concerned?

16. Do you use any authentication mechanism on your device? Examples include a password, pattern or PIN. Why or why not?
    (a) What is protected by the authentication? (Simcard? Phone?)
    (b) What strategies did you use to create this authentication scheme?
    (c) How did you learn about this? Did you get any advice?

Miscellaneous

17. Is there anything else you would like to share about cybercafes?

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

18. Do you own a computer or laptop?
19. What is your age?
20. What is your gender?
21. Are you employed?
22. What is the highest level of education you have attained?
23. Do you have a background in IT or computers as part of your work experience or school? If so, please explain.
24. Do you have any feedback or questions about this interview?

B.2 Codebook

- **cybercafe-establishment/work-reason (17)**
  business-opportunity (10), computer-interest (4), relevant-skills (3)
- **manager-cybercafe-experience (14)**
  1-5-years (9), less-than-a-year (3), 6-10-years (1), over-10-years (1)
- **cybercafe-number-of-computers (14)**
  1-5-computers (8), 6-10-computers (5), over-10-computers (1)
- **cybercafe-number-of-printers (14)**
  2-printers (8), 1-printer (3), 3-printers (2), 4-printers (1)
- **OS-type/software (16)**
  windows (14), cybercafe-pro (2)
- **update-OS (19)**
  yes (11): *automatic (5), improve-speed/performance (3), get-new-features (1), follow-latest-trends (1)*
  no (8): *users-familiar-with-old-OS (2), not-concerned-about-security (2), updates-slow-machines (1), updates-consume-space (1), inconveniencing-reboots (1), updates-consume-data (1)*
- **cybercafe-customer-positives (44)**
  equipment-availability (12), faster-internet (11), affordability (5), availability-of-assistance (5), privacy (4), stable-electricity (2), meet-friends/social-place (2), conveniently-located (2), ample-space (1)
- **cybercafe-customer-negatives (11)**
  unhelpful/unfriendly-managers (3), crowded/have-queues (3), noisy-cybers (3), many-advertisements (1), expensive (1)

- **factors-when-choosing-cybercafe (51)**
  conducive-environment (9), internet-speed (7), manager-friendliness/assistance (7), cost/affordability (7), location/proximity (5), state/number/speed-of-equipment (4), space-availability (4), electricity-stability (3), safety (3), privacy (2)
- **cybercafe-challenges (55)**
  slow-internet (20), electricity-outage (9), old/faulty-equipment (6), payment-issues-with-customers (5), slow-hanging-machines (4), government/law-enforcement-harassment (4), expensive-equipment (3), few-customers (2), drunk/rowdy-customers (2)
- **cybercafe-common-services (132)**
  printing (18), eCitizen (18), job-applications (13), email (10), photocopy (9), assignments/school-projects (9), document-typing/editing (8), school/HELB/scholarship-applications (7), social-media (7), work/online-work (5), KRA/taxes (5), movie-streaming/download (4), gambling (4), lamination (4), computer-training (3), scanning (3), search/Google (3), visa-applications (2), graphic-design (2)
- **other-services-offered-at-cybercafes (16)**
  sell-computers/phones (5), gaming (3), banking-services (2), mobile-money (2), repairs (2), computer-networking (1), passport-photos (1)
- **services-not-offered (15)**
  forgery (5): *have-intergrity (2), fear-consequences (2)*
  web-design (3): *lack-time/skills (3)*
  music-download (2): *illegal/not-licensed (2)*
  rooting/phone-formatting (1): *lack-time/skills (1)*
  photography (1): *different-business (1)*
  bulk-printing (1): *lack-equipment (1)*
  passport-photo-printing (1): *lack-equipment (1)*
  lamination/binding (1): *lack-equipment (1)*
- **customer-common-challenges (77)**
  computer-usage (30): *challenges-printing/binding/scanning (6), using-programs/apps (6), navigating-websites/computers (5), struggle-typing (2), difficulty-opening-flashdisks (1)*

  difficulty-accessing/recovering-account (26): *forgot-password (12), forgot-email/lost-phone (9), bad-UI/UX (2), website-downtime (1)*

  account-setup (7): *difficulty-complying-with-password-requirements (2), users-don't-care-about-password (1), don't-know-password-to-use (1), don't-know-what-to-do (1)*

  information-retrieval (2): *website-in-foreign-language (1)*

  customers-fear-computers (1), customers-sent-but-forgot-details (1)

  not-faced-challenges (10) *specific-tasks/cybercafes (4), experienced-with-computers (3), tasks-easy (2), availability-of-assistance (1)*
- **customers-ask-for-help (23)**
- **customers-satisfied-with-help (14)**
  yes (8): *issue-resolved (5), answers-satisfactory (1), not-compromised (1)*
  no (6): *took-long (2), challenge-unresolved (2), guidance-not-provided (1), spent-more-money (1)*
- **advice/support-offered-to-customers (69)**
  password-and-account-management (38): use-memorable-password (13): *combination-of-ID/name/birthday (5), use-ID-number (4), use-birthday (1), use-phone-number (1)*
  account-management-for-customers (10): *save/manage-user-password (3), select-password-for-customer (3), standard-email-account-for-customers (1), avoid-selecting-password-for-customer (1), use-phone-number-of-manager (1)*
  use-strong-password (4): *mixed-characters (2)*
  don't-save-password-in-browser (3) avoid-common-passwords (2) password-protect-files (1) use-secret-password (1) frequently-change-password (1) save-password-in-browser (1)

do-task-for-customer (7): *tasks-technical (1)*
teach/guide-customers (7), *account-recovery (5)*, *logout (3)*, *use-phone-number-for-accounts (2)*, *update-OS (1)*, *don't-save-files-on-desktop (1)*, *avoid-clicking-on-links (1)*, *use-another-computer (1)*
no-security-advice-offered (1): *manager-interested-in-money (1)* **don't-interrupt/help-customers (1):** *make-more-money (1)*

- **unresolved/difficult-challenges (11)**
account-recovery (8): *forgot-email/lost-phone (8)*
edit-pdfs (1), *edit-photos (1)*, *disabling-forgotten-password (1)*
- **question-manager-has-no-answer (11)**
research (4), say-don't-know (3), refer-customer-to-other-cybers (3)
- **sources-of-advice (62)**
internet (27), personal-experience (12), managers/other-managers (8), friends/family (6), customer-service (1), tv-shows (1)
- **customers-follow-advice (45)**
yes (33): *works/good-advice (10), protect-themselves/info (7), trust-manager (4), view-manager-as-expert/knowledgeable (3), limited-time/task-urgent (3), manager-friendly/engaging (2), heard-similar-advice (1), interested-in-computers (1), solve-issues-in-future (1)*
no (12): *contradictory-beliefs (2), elderly (2), think-manager-lying/skeptical (2), too-technical (1), don't-have-time (1), will-make-them-spend-more-money (1), been-advised-differently (1), many-emails-criminal (1), task-not-urgent (1)*
- **top-three-advice-to-stay-safe (108)**
logout (12), avoid-links/malicious-sites (11), strong/secure-passwords (10), don't-save-passwords (9), use-a-password (6), don't-share-passwords (5), avoid-public-wifi (4), unique-passwords (4), firewall (3), multi-factor-authentication (3), clear-history (3), being-aware (3), delete-downloads (2), use-safe-browser (2), anti-virus (2), avoid/skip-links (2), close-websites (1), clear-cache (1), use-phone-number-for-recovery (1), block/avoid-unsafe-sites (1), faster-internet (1), use-cctv (1), avoid-unknown-downloads (1), incognito-mode (1), don't-sync-with-browser (1), block-cookies (1), update-system (1), prevent-idleness (1), browser-in-safe-environment (1), follower-cybercafe-guidelines (1), avoid-unsafe-cybercafes (1), avoid-common-passwords (1), use-data-saver (1), keep-username-secret (1), don't-save-to-desktop (1), stick-to-first-google-result (1), disable-notifications (1), frequently-change-password (1), limit-info-shared-online (1), limit-online-interactions (1), computer-knowledge (1), stick-to-one-cybercafe (1)
- **follow-top-three-advice (38)**
yes (29): *stay-safe (4)*
sometimes/some (9): *usability-vs-security (3), not-offered/required (2), time-consuming (1), enough-data (1), forget (1)*
- **top-three-advice-offered-to-customers (25)**
logout (5), don't-save-passwords (3), avoid-links/malicious-sites (2), strong-passwords (2), being-aware (2), 2FA (1), use-a-password (1), incognito-mode (1), delete-files/downloads (1), don't-sync-with-browser (1), avoid-public-wifi (1), block-cookies (1), update-system (1), firewall (1), use-safe-browser (1)
- **not-following-top-three-advice (83)**
susceptible-to-attacks/compromises (25): *virus (7), hacking (4), impersonation (2), malware (1), ransomware (1)*
unauthorized-access (16), data-leaks/loss/manipulation (11), financial-loss/fraud (8), monitoring/surveillance (5), loss-of-account-access (2), theft-of-equipment (2), identity-theft (2), slow-internet (2), miss-features (2), unnecessary-pop-ups/ads (1), access-insecure-sites (1), don't-know (1), bans-from-cyber (1), device-failure (1), more-data (1), waste-time (1), get-distracted (1)
- **security/privacy-concerns (86)**
concerns-about/for-customers (30): *access-porn/illegal-sites (7), scams/fraud (5), theft-of-equipment*

(4), download-prohibited-equipment (4), identity-theft(3), easy-passwords (2), physical-damage (2), malicious-activities (2), install/tamper-with-OS (1)
hacking/account-take-over (15): *money-loss (6), impersonation (4)*
unauthorized-access-of-account/info (14): *cyber-bullying (2), disable-partner's-accounts (1), black-mail (1)*
leaving-data-in-cybercafe (9), data-theft/manipulation (5), lack-of-privacy (3), shoulder-surfing (2), spyware/tracking (2), saving-passwords-in-cybers (2), over-sharing-info (2), forgery (1)
no-concerns (1): *used-to-the-internet (1)*

- **security/privacy-standard-practices (78)**
  at-end-of-user-session (30)
  logout-customer (13): *prevent-malicious-use (5), prevent-unauthorized-access (2), increase-trust (1)*
  clear-downloads (9): *prevent-malicious-use (2), space-constraints (2), protect-private-info (2), legal-liability (1)*
  reset/end-user-session (4), sanitize-equipment (1), check-history/downloads (1), sleep-computer (1), close-sites (1)
  other-standard-practices (39): *partitions-for-privacy (5), block-sites (5), anti-virus (4), block-flash/USB (3), warning/notes (2), dusting (2), disabled-illegal-downloads (2), inspect-files/block-software-installation (2), prevent-idleness (2), monitor-kids (2), safely-store-customer-docs (1), lock-doors (1), chain-equipment (1), firewall (1), format-computers (1), strong-passwords-for-cyber-computers (1), outsource-servicing (1), delete-saved-passwords (1), use-vpn (1), delete-saved-passwords/history (1)*
- **customer-end-of-session-activities (35)**
  logout (20): *prevent-unauthorized-access (14), cyber-directives (2)*
  clear-history (5), clear-downloads (4), don't-save-password (2), close-websites (2), shutdown (1)
- **customer-and-manager-suggestions (4)**
  need-for-computer-education (4)

Appendix C: Security and Privacy Advice in the Majority World

C.1 Interview Script

Local Experts' Background

1. Please tell me a little bit about yourself and what you do.
2. Can you briefly describe the area you live in in [country x]?
   (a) Is it rural or urban?
3. Are there any general challenges around technology and/or its use in [country x] that you are aware of? Please elaborate.
4. What role do you play in supporting people with their technology challenges/needs in [country x]?
   (a) How would you characterize the types of people who come to you?
   (b) How do you think people get to know about you or come to find you?
   (c) Why do you think they specifically come to you?
   (d) What is the biggest challenge that most people you support face?
   (e) What advice or support do you provide them in resolving these challenges?
   (f) Are these challenges always resolved? What challenges are particularly difficult to resolve?
5. What other sources do people in your area/country/community use to obtain technology support?

Security and Privacy Concerns: Personal

6. Personally, do you have any concerns relating to technology or how you use technology in general? Please elaborate.
   (a) What factors do you think influence these concerns? Prompts: The type of technology you use, where you access the technology from etc.
   (b) Do any of these concerns specifically relate to security and privacy?
   (c) How do you handle these concerns?

Security and Privacy Concerns: About Others

7. What concerns relating to the usage of technology that people from your community or [country x] come to you with? Please elaborate.
   (a) Have you noticed any patterns in terms of the types of people who express certain concerns more than others? For example, do older people tend to have different concerns than younger people? What about gender?
   (b) Are there other concerns people come to you, particularly about security or privacy?
   (c) How do you handle (or help them handle) these concerns?

Security and Privacy Advice

8. What are the 3 top things you do (or would) to protect your digital security and privacy?
   For each piece of advice:
   (a) Where did you learn about this advice?
   (b) Do you follow this advice?

(c) Have you faced any challenges following this advice? Please elaborate.

9. Have you provided any advice to those in your local community or [country x] to protect their digital security and privacy?
If yes:

   (a) What are the top 3 pieces of advice you have provided to those you support in your local community or in [country x] to protect their security and privacy?
   For each piece of advice:

      i. Where did you learn about this piece of advice?
      ii. Why do you think this advice is important for these users?
      iii. What challenges do people face in following this advice?
      iv. Do you vary this advice based on the target users? Prompts: different identities, skills, resources etc. Please elaborate.

If no:

   (a) What are the top 3 pieces of advice you would give to those you support in your local community or in [country x] to protect their security and privacy?
   For each piece of advice:

      i. Where did you learn about this piece of advice?
      ii. Why do you think this advice is important for these users?
      iii. What challenges do you think people would face in following this advice?
      iv. Would you vary this advice based on the target users? Prompts: different identities, skills, resources etc. Please elaborate.

10. Is there any advice you would love to give but cannot provide? Why?
11. What gaps or opportunities for improvement do you see for security and privacy advice in your local community or [country x]? Please elaborate.

Security and Privacy Practices: Personal

12. Personally, how do you most frequently access the Internet?
13. What are the technologies, devices or services that you regularly use? Prompts: smartphone, computer, social media, mobile money etc.

   (a) In what contexts/for what purposes do you use these devices or services? For example at work or at home?

   (b) Do you share any of these devices or services with others? With whom and why?

   (c) Do you have any concerns about other people having access to these devices or services? Why or why not?

14. For the mentioned devices, do you have any standard security and privacy practices?

   (a) How often do you update your OS? Why or why not?

   (b) Do you use any antivirus software? Why or why not?

   (c) How do you generally select and manage passwords across different websites? Do you use any password managers?

   (d) Do you use multifactor authentication for any sites? Why or why not?

   (e) Do you use any password/PIN/pattern on your devices?

Security and Privacy Practices: About Others

15. For the people you assist (or have assisted), how do they mostly access the Internet (if they do)?
    (a) Do they face any challenges with this?
    (b) Do any of them use public computers? For what purposes?
16. For the people that you most frequently support, what technologies, devices or services do they regularly use? Prompts: smartphones, computers, social media, mobile money etc.
    (a) In what contexts/for what purposes do you think they mostly use these devices or services?
    (b) Do you know if they share these devices or services with others? Why?
17. Are you aware of any standard security and privacy practices that these users may have for these devices or services?
    (a) How often do they update the OS for their devices? Why or why not?
    (b) Do they use any antivirus software on their devices? Why or why not?
    (c) How do they generally select and manage passwords across different sites? Do they use any password managers?
    (d) Do they use multifactor authentication for any sites? Why or why not?

Other Challenges

18. Are any services in [country x], for example government services, digitized?
    (a) Please provide examples of these services.
    (b) How do you personally access these services?
    (c) How do most people (including those you support) access these services?
    (d) What are some of the challenges people face in accessing these services?
19. Are you aware of any common scams or phishing schemes in [country x]?
    (a) Please provide examples.
    (b) Have you (or anyone you know or assist) fallen for these?
    (c) How can users in [country x] protect themselves from these scams? Have you provided this advice to any users?
20. Do you feel digitally surveilled in [country x]? Please elaborate.
    (a) Who is responsible for this surveillance?
    (b) Are people (including those you support) concerned about this?
    (c) Do you use any techniques to protect yourself?
    (d) What advice (if any) would you give to other users to (potentially) protect themselves with regards to the stated surveillance?
21. Are any sites, apps or platforms banned or blocked in [country x]?
    (a) Please provide examples of these sites or platforms.
    (b) Who has blocked these services?
    (c) What workarounds are people (including those you support) using, if any?
    (d) Are you personally using any workarounds?

Demographic Questions

22. What is your age?
23. With which gender do you most identify with?
24. What is the highest level of education you have attained?
25. What is your occupation/profession?

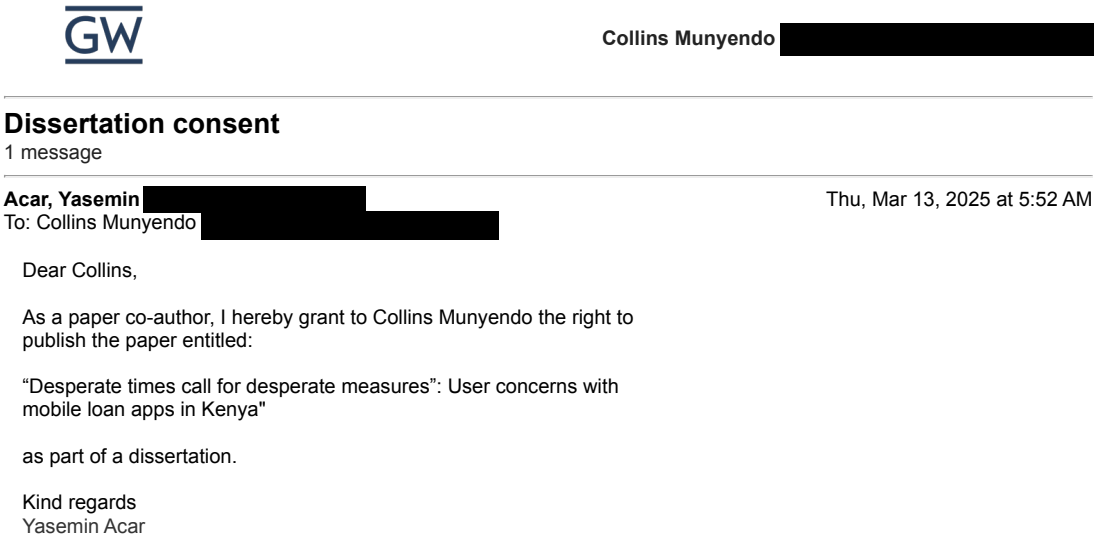
Appendix D: Copyright Permissions

This appendix contains the copyright information for the three previously published papers [102, 103, 106] used in this dissertation. These papers were published at the IEEE Symposium on Security and Privacy. The IEEE Symposium on Security and Privacy consent form for refereed papers (see below) recognizes the author(s) as retaining ownership of the Work including:

1. Author(s), or their employers, retaining all proprietary rights in any process, procedure, or article of manufacture described in the Work.
2. In the case of work performed under a U.S. Government contract or grant, IEEE recognizes that the U.S. Government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official U.S. Government purposes only, if the contract/grant so requires.

The right to publish statements in emails from co-authors for previously published works is also included.

D.1 Mobile Loan Apps (IEEE S&P 2022)



GW

Collins Munyendo [redacted]

Dissertation consent
1 message

Acar, Yasemin [redacted] Thu, Mar 13, 2025 at 5:52 AM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper entitled:

“Desperate times call for desperate measures”: User concerns with mobile loan apps in Kenya"

as part of a dissertation.

Kind regards
Yasemin Acar

Figure D.1: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent

1 message

Adam Aviv [redacted] Thu, Mar 13, 2025 at 9:29 AM
To: "Munyendo, Collins" [redacted]

Dear Collins,

As a paper co-author, I hereby grant you, Collins Munyendo, the right to publish the papers entitled:

"In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya"

and

“Desperate times call for desperate measures”: User concerns with mobile loan apps in Kenya"

as part of your dissertation.

Best,

-adam

Figure D.2: Email Containing a Right To Publish Statement.

IEEE COPYRIGHT LICENSE FORM
FOR USE WITH IEEE COMPUTER SOCIETY'S
EXPERIMENTAL "DELAYED-OPEN ACCESS" MODEL

TITLE OF WORK (hereinafter, "the Work"): "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya

AUTHOR(S): Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv

IEEE PUBLICATION TITLE: 2022 IEEE Symposium on Security and Privacy (SP)

The undersigned hereby grants to The Institute of Electrical and Electronics Engineers, Incorporated ("IEEE") an exclusive, worldwide, royalty free license to reproduce, distribute, sell, make derivative works of, and use the Work, for a period of twelve (12) months from the date of the execution of this agreement and inclusion of the paper in the IEEE Xplore Digital Library. Upon the conclusion of this exclusivity period, IEEE shall retain all rights previously granted on a non-exclusive basis in perpetuity. IEEE shall also make the Work available at no cost through IEEE's digital library upon the conclusion of the exclusivity period.

The author(s) represents and warrants that the Work is original and that he/she/they is/are the author(s) of the Work. To the extent required, the Author(s) represent and warrant that they have obtained all necessary permissions from any third party intellectual property owners. The author(s) further represent that they have the power and authority to make and execute this agreement.

IEEE recognizes the author(s) as retaining ownership of the Work including:

1. Author(s), or their employers, retaining all proprietary rights in any process, procedure, or article of manufacture described in the Work.

2. In the case of work performed under a U.S. Government contract or grant, IEEE recognizes that the U.S. Government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official U.S. Government purposes only, if the contract/grant so requires.

The author(s) hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work, and releases IEEE from any claim based on right of privacy or publicity.

The author(s) agree to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.

In the event the above Work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, this agreement becomes null and void.

AUTHOR

04/06/2022

DATE

JOINT AUTHORSHIP

For jointly authored works, all the joint authors should sign, or one of the authors should sign as an authorized agent for the others. In the case of multiple authorship where one or more authors are U.S. Government employees but at least one author is not, that non-Government author should sign this form.

TERMS & CONDITIONS and RETAINED RIGHTS

General

1. Authors whose work was performed under a grant from a funding agency are free to fulfill any deposit mandates from that funding agency.

Author Online Use of Open Access Articles

2. Classroom or Internal Training Use. An author is expressly permitted to post any portion of the final, published version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.

INFORMATION FOR AUTHORS

Author Responsibilities: The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html. Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

Author/Employer Rights: If you are employed and prepared the Work on a subject within the scope of your employment, the copyright in the Work belongs to your employer as a work-for-hire. In that case, the IEEE assumes that when you sign this Form, you are authorized to do so by your employer and that your employer has consented to the representation and warranty of publication rights and to all other terms and conditions of this Form. If such authorization and consent has not been given to you, an authorized representative of your employer should sign this Form as the Author.

Content Distribution: The IEEE distributes its technical publications throughout the world and does so by various means such as hard copy, microfiche, microfilm, and electronic media. It also abstracts and may translate its publications, and articles contained therein, for inclusion in various compendiums, collective works, databases and similar publications.

Authors may, as permitted by standard IEEE copyright policy, post the as-accepted version of the Work on their personal and/or institutional websites. After the expiration of this license, Authors may post the as-published version of the Work on such sites, with the exception of any interactive version developed by IEEE. Authors are not restricted from producing their own, independently derived interactive works.

INFORMATION FOR READERS ON THE USE OF OPEN ACCESS ARTICLES

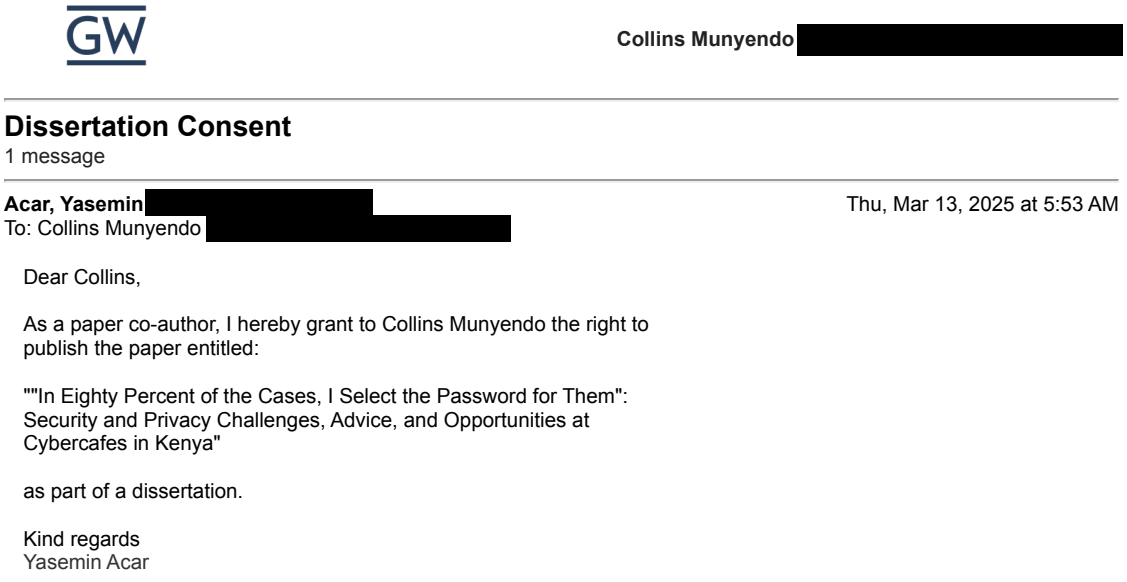
Reuse: Third-party users may view, print, copy and download the content for personal use or academic purposes. Users may also post links to the published IEEE version of the Work, including the Digital Object Identifier (DOI), for their own non-commercial use. All third-party users must provide complete attribution to both the IEEE publication title and the names of the author(s) of the Work. To copy otherwise, or to distribute/display the Work by third parties, requires the permission of IEEE.

Reserved Rights of IEEE: IEEE reserves the right to limit the production of derivative works and commercial exploitation of the Work for the duration of this license (12 months from the initial posting date in the IEEE Xplore Digital Library). Should a third party seek to make a derivative work based on the Work or commercially exploit the Work during this period they must seek permission from IEEE.

Text and Data Mining/Translation Rights: Non-commercial translations as well as text and data mining of the Work are permitted. However, during the licensing period, should a third party seek to engage in such activity for commercial purposes the express, written permission of IEEE shall be required. Any translation must prominently link to the IEEE published version and prominently display the following: "This is an unofficial translation of an IEEE publication. IEEE has not endorsed the content of this translation."

THIS FORM MUST ACCOMPANY THE SUBMISSION OF THE AUTHOR'S MANUSCRIPT.
Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966

D.2 Cybercafes (IEEE S&P 2023)



GW

Collins Munyendo [redacted]

Dissertation Consent
1 message

Acar, Yasemin [redacted] Thu, Mar 13, 2025 at 5:53 AM
To: Collins Munyendo [redacted]

Dear Collins,

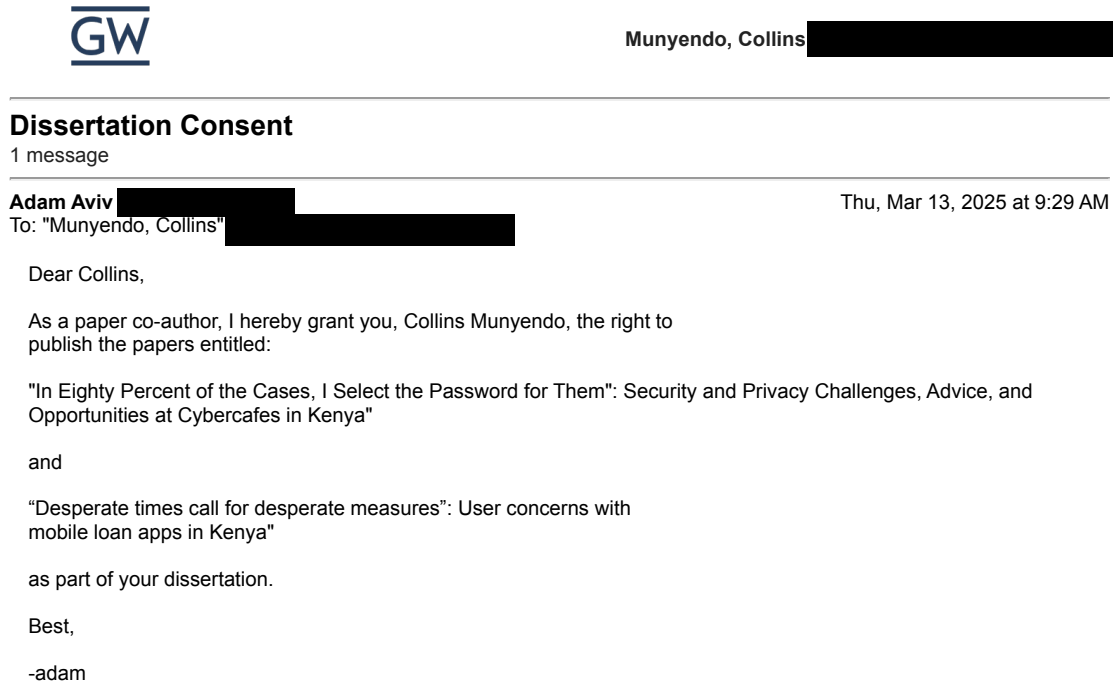
As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper entitled:

""In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya"

as part of a dissertation.

Kind regards
Yasemin Acar

Figure D.3: Email Containing a Right To Publish Statement.



GW

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Adam Aviv [redacted] Thu, Mar 13, 2025 at 9:29 AM
To: "Munyendo, Collins" [redacted]

Dear Collins,

As a paper co-author, I hereby grant you, Collins Munyendo, the right to publish the papers entitled:

"In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya"

and

“Desperate times call for desperate measures”: User concerns with mobile loan apps in Kenya"

as part of your dissertation.

Best,

-adam

Figure D.4: Email Containing a Right To Publish Statement.

IEEE COPYRIGHT LICENSE FORM
FOR USE WITH IEEE COMPUTER SOCIETY'S
EXPERIMENTAL "DELAYED-OPEN ACCESS" MODEL

TITLE OF WORK (hereinafter, "the Work"): "In Eighty Percent of the Cases, I select the Password for Them": Security and Privacy Challenges, Advice and Opportunities at Cybercafes in Kenya

AUTHOR(S): Collins W. Munyendo, Yasemin Acar, and Adam J. Aviv

IEEE PUBLICATION TITLE: 2023 IEEE Symposium on Security and Privacy (SP)

The undersigned hereby grants to The Institute of Electrical and Electronics Engineers, Incorporated ("IEEE") an exclusive, worldwide, royalty free license to reproduce, distribute, sell, make derivative works of, and use the Work, for a period of twelve (12) months from the date of the execution of this agreement and inclusion of the paper in the IEEE Xplore Digital Library. Upon the conclusion of this exclusivity period, IEEE shall retain all rights previously granted on a non-exclusive basis in perpetuity. IEEE shall also make the Work available at no cost through IEEE's digital library upon the conclusion of the exclusivity period.

The author(s) represents and warrants that the Work is original and that he/she/they is/are the author(s) of the Work. To the extent required, the Author(s) represent and warrant that they have obtained all necessary permissions from any third party intellectual property owners. The author(s) further represent that they have the power and authority to make and execute this agreement.

IEEE recognizes the author(s) as retaining ownership of the Work including:

1. Author(s), or their employers, retaining all proprietary rights in any process, procedure, or article of manufacture described in the Work.

2. In the case of work performed under a U.S. Government contract or grant, IEEE recognizes that the U.S. Government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official U.S. Government purposes only, if the contract/grant so requires.

The author(s) hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work, and releases IEEE from any claim based on right of privacy or publicity.

The author(s) agree to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.

In the event the above Work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, this agreement becomes null and void.

Collins W. Munyendo
_____
AUTHOR

03/29/2023
_____
DATE

JOINT AUTHORSHIP

For jointly authored works, all the joint authors should sign, or one of the authors should sign as an authorized agent for the others. In the case of multiple authorship where one or more authors are U.S. Government employees but at least one author is not, that non-Government author should sign this form.

TERMS & CONDITIONS and RETAINED RIGHTS

General

1. Authors whose work was performed under a grant from a funding agency are free to fulfill any deposit mandates from that funding agency.

Author Online Use of Open Access Articles

2. Classroom or Internal Training Use. An author is expressly permitted to post any portion of the final, published version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.

INFORMATION FOR AUTHORS

Author Responsibilities: The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html. Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

Author/Employer Rights: If you are employed and prepared the Work on a subject within the scope of your employment, the copyright in the Work belongs to your employer as a work-for-hire. In that case, the IEEE assumes that when you sign this Form, you are authorized to do so by your employer and that your employer has consented to the representation and warranty of publication rights and to all other terms and conditions of this Form. If such authorization and consent has not been given to you, an authorized representative of your employer should sign this Form as the Author.

Content Distribution: The IEEE distributes its technical publications throughout the world and does so by various means such as hard copy, microfiche, microfilm, and electronic media. It also abstracts and may translate its publications, and articles contained therein, for inclusion in various compendiums, collective works, databases and similar publications.

Authors may, as permitted by standard IEEE copyright policy, post the as-accepted version of the Work on their personal and/or institutional websites. After the expiration of this license, Authors may post the as-published version of the Work on such sites, with the exception of any interactive version developed by IEEE. Authors are not restricted from producing their own, independently derived interactive works.

INFORMATION FOR READERS ON THE USE OF OPEN ACCESS ARTICLES

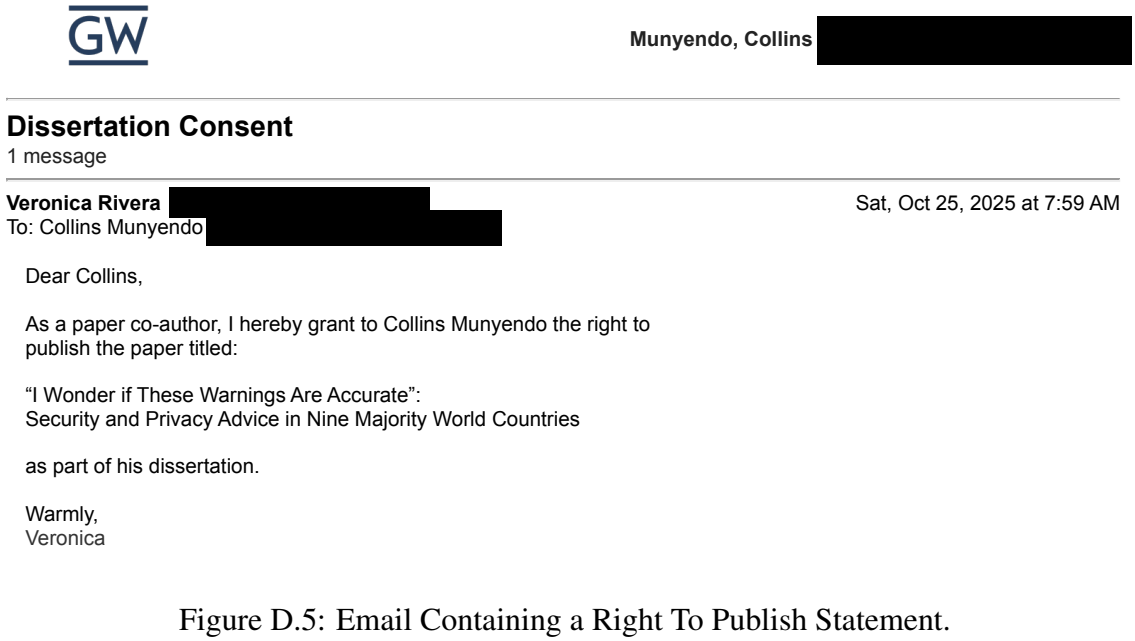
Reuse: Third-party users may view, print, copy and download the content for personal use or academic purposes. Users may also post links to the published IEEE version of the Work, including the Digital Object Identifier (DOI), for their own non-commercial use. All third-party users must provide complete attribution to both the IEEE publication title and the names of the author(s) of the Work. To copy otherwise, or to distribute/display the Work by third parties, requires the permission of IEEE.

Reserved Rights of IEEE: IEEE reserves the right to limit the production of derivative works and commercial exploitation of the Work for the duration of this license (12 months from the initial posting date in the IEEE Xplore Digital Library). Should a third party seek to make a derivative work based on the Work or commercially exploit the Work during this period they must seek permission from IEEE.

Text and Data Mining/Translation Rights: Non-commercial translations as well as text and data mining of the Work are permitted. However, during the licensing period, should a third party seek to engage in such activity for commercial purposes the express, written permission of IEEE shall be required. Any translation must prominently link to the IEEE published version and prominently display the following: "This is an unofficial translation of an IEEE publication. IEEE has not endorsed the content of this translation."

THIS FORM MUST ACCOMPANY THE SUBMISSION OF THE AUTHOR'S MANUSCRIPT.
Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966

D.3 Security and Privacy Advice in the Majority World (IEEE S&P 2026)



GW

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Veronica Rivera [redacted] Sat, Oct 25, 2025 at 7:59 AM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Warmly,
Veronica

Figure D.5: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Jackie Hu [redacted] Sat, Oct 25, 2025 at 6:34 AM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant you (Collins Munyendo) the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of your dissertation. (And honestly I don’t think you need my permission as you clearly did the bulk of work and all the heavy lifting. Congratulations again on your dissertation!)

Best,
Jackie

Jackie Hu
PhD Student, School of Information
University of Michigan

Figure D.6: Email Containing a Right To Publish Statement.

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Emmanuel Tweneboah [redacted] Fri, Oct 24, 2025 at 4:48 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”: Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards

Emmanuel Tweneboah

Figure D.7: Email Containing a Right To Publish Statement.

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Amna Shahnawaz [redacted] Fri, Oct 24, 2025 at 3:08 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards
Amna Shahnawaz

Figure D.8: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent

1 message

Sowon, Karen Cheruto [redacted] Mon, Oct 27, 2025 at 11:33 AM
To: "cmunyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards
Karen

Figure D.9: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent

1 message

Dilara Kekulluoglu [redacted] Fri, Oct 24, 2025 at 2:41 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Best,
Dilara Keküllüoğlu

Figure D.10: Email Containing a Right To Publish Statement.

Collins Munyendo [redacted]

Dissertation Consent

1 message

Marcos Silva [redacted] Fri, Oct 24, 2025 at 3:22 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards,
Marcos Silva

Figure D.11: Email Containing a Right To Publish Statement.

Munyendo, Collins [redacted]

Dissertation Consent

1 message

yue.deng [redacted] Mon, Oct 27, 2025 at 1:46 AM
To: "cmunyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to

publish the paper titled:

“I Wonder if These Warnings Are Accurate”:

Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Best,

Yue

Figure D.12: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

DISSERTATION CONSENT

1 message

MERCY OMEIZA [redacted] Mon, Oct 27, 2025 at 12:24 PM
To: cmunyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards

Figure D.13: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent

1 message

Gayatri Priyadarsini [redacted] Fri, Oct 24, 2025 at 2:31 PM
To: [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Regards,
Gayatri Priyadarsini Kancherla
IIT Gandhinagar, India

Figure D.14: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Right to publish the paper: “I wonder of These Warning Are Accurste”
1 message

Rosario Niniz [redacted] Tue, Oct 28, 2025 at 12:01 AM
To: "cmunyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards

María Rosario Niniz Silva

Figure D.15: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation consent
1 message

Abhishek Bichhawat [redacted] Mon, Oct 27, 2025 at 11:16 AM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards

-- Abhishek

Figure D.16: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

[S&P 2026 Cycle 1] Updated accepted #70 ""I Wonder if These Warnings Are..."

Maryam Mustafa [redacted] Mon, Oct 27, 2025 at 1:21 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards
Maryam Mustafa

Figure D.17: Email Containing a Right To Publish Statement.

GW

Munyendo, Collins [redacted]

Dissertation Consent
1 message

Marmolejo Cossio, Francisco [redacted] Fri, Oct 24, 2025 at 2:53 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Best regards,
Francisco

Figure D.18: Email Containing a Right To Publish Statement.

Collins Munyendo [redacted]

Dissertation consent

1 message

Elissa Redmiles [redacted] Fri, Oct 24, 2025 at 2:23 PM
To: Collins Munyendo [redacted]

As a paper co-author, I hereby grant to Collins Munyendo the right to
publish the paper titled:“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countriesas part of his dissertation.

Smiles,
Elissa

--
Elissa Redmiles
Clare Luce Boothe Assistant Professor of Computer Science
Georgetown University
[redacted]

Figure D.19: Email Containing a Right To Publish Statement.

Munyendo, Collins [redacted]

Dissertation consent

1 message

Yixin Zou [redacted] Fri, Oct 24, 2025 at 2:11 PM
To: Collins Munyendo [redacted]

Dear Collins,

As a paper co-author, I hereby grant to Collins Munyendo the right to publish the paper titled:

“I Wonder if These Warnings Are Accurate”:
Security and Privacy Advice in Nine Majority World Countries

as part of his dissertation.

Kind regards
Yixin

Figure D.20: Email Containing a Right To Publish Statement.

IEEE COPYRIGHT LICENSE FORM
FOR USE WITH IEEE COMPUTER SOCIETY'S
EXPERIMENTAL "DELAYED-OPEN ACCESS" MODEL

TITLE OF WORK (hereinafter, "the Work"): "I Wonder if These Warnings Are Accurate": Security and Privacy Advice in Nine Majority World Countries

AUTHOR(S): Collins W. Munyendo, Veronica A. Rivera, Jackie Hu, Emmanuel Tweneboah, Amna Shahnawaz, Karen Sowon, Dilara Kekulluoglu, Marcos Silva, Yue Deng, Mercy Omeiza, Gayatri Priyadarsini Kancherla, Maria Rosario Niniz Silva, Abhishek Bichhawat, Maryam Mustafa, Francisco Marmolejo-Cossio, Elissa M. Redmiles, and Yixin Zou

IEEE PUBLICATION TITLE: 2026 IEEE Symposium on Security and Privacy (SP)

The undersigned hereby grants to The Institute of Electrical and Electronics Engineers, Incorporated ("IEEE") an exclusive, worldwide, royalty free license to reproduce, distribute, sell, make derivative works of, and use the Work, for a period of twelve (12) months from the date of the execution of this agreement and inclusion of the paper in the IEEE Xplore Digital Library. Upon the conclusion of this exclusivity period, IEEE shall retain all rights previously granted on a nonexclusive basis in perpetuity. IEEE shall also make the Work available at no cost through IEEE's digital library upon the conclusion of the exclusivity period.

The author(s) represents and warrants that the Work is original and that he/she/they is/are the author(s) of the Work. To the extent required, the Author(s) represent and warrant that they have obtained all necessary permissions from any third party intellectual property owners. The author(s) further represent that they have the power and authority to make and execute this agreement.

IEEE recognizes the author(s) as retaining ownership of the Work including:

1. Author(s), or their employers, retaining all proprietary rights in any process, procedure, or article of manufacture described in the Work.

2. In the case of work performed under a U.S. Government contract or grant, IEEE recognizes that the U.S. Government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official U.S. Government purposes only, if the contract/grant so requires.

The author(s) hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work, and releases IEEE from any claim based on right of privacy or publicity.

The author(s) agree to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.

In the event the above Work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, this agreement becomes null and void.

__Collins W. Munyendo_____
AUTHOR

___10/18/2025_____
DATE

JOINT AUTHORSHIP

For jointly authored works, all the joint authors should sign, or one of the authors should sign as an authorized agent for the others. In the case of multiple authorship where one or more authors are U.S. Government employees but at least one author is not, that non-Government author should sign this form.

TERMS & CONDITIONS and RETAINED RIGHTS

General

1. Authors whose work was performed under a grant from a funding agency are free to fulfill any deposit mandates from that funding agency.

Author Online Use of Open Access Articles

2. Classroom or Internal Training Use. An author is expressly permitted to post any portion of the final, published version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.

INFORMATION FOR AUTHORS

Author Responsibilities: The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html. Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

Author/Employer Rights: If you are employed and prepared the Work on a subject within the scope of your employment, the copyright in the Work belongs to your employer as a work-for-hire. In that case, the IEEE assumes that when you sign this Form, you are authorized to do so by your employer and that your employer has consented to the representation and warranty of publication rights and to all other terms and conditions of this Form. If such authorization and consent has not been given to you, an authorized representative of your employer should sign this Form as the Author.

Content Distribution: The IEEE distributes its technical publications throughout the world and does so by various means such as hard copy, microfiche, microfilm, and electronic media. It also abstracts and may translate its publications, and articles contained therein, for inclusion in various compendiums, collective works, databases and similar publications.

Authors may, as permitted by standard IEEE copyright policy, post the as-accepted version of the Work on their personal and/or institutional websites. After the expiration of this license, Authors may post the as-published version of the Work on such sites, with the exception of any interactive version developed by IEEE. Authors are not restricted from producing their own, independently derived interactive works.

INFORMATION FOR READERS ON THE USE OF OPEN ACCESS ARTICLES

Reuse: Third-party users may view, print, copy and download the content for personal use or academic purposes. Users may also post links to the published IEEE version of the Work, including the Digital Object Identifier (DOI), for their own non-commercial use. All third-party users must provide complete attribution to both the IEEE publication title and the names of the author(s) of the Work. To copy otherwise, or to distribute/display the Work by third parties, requires the permission of IEEE.

Reserved Rights of IEEE: IEEE reserves the right to limit the production of derivative works and commercial exploitation of the Work for the duration of this license (12 months from the initial posting date in the IEEE Xplore Digital Library). Should a third party seek to make a derivative work based on the Work or commercially exploit the Work during this period they must seek permission from IEEE.

Text and Data Mining/Translation Rights: Non-commercial translations as well as text and data mining of the Work are permitted. However, during the licensing period, should a third party seek to engage in such activity for commercial purposes the express, written permission of IEEE shall be required. Any translation must prominently link to the IEEE published version and prominently display the following: "This is an unofficial translation of an IEEE publication. IEEE has not endorsed the content of this translation."

THIS FORM MUST ACCOMPANY THE SUBMISSION OF THE AUTHOR'S MANUSCRIPT.
Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966