CO-oPS: A Mobile App for Community Oversight of Privacy and Security

Poster · September 2022

DOI: 10.1145/3500868.3559706

8 authors, including:

Mamtaj Akter
Vanderbilt University
8 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Nazmus Sakib Miazi
University of North Carolina at Charlotte
8 PUBLICATIONS **88** CITATIONS
SEE PROFILE

Pamela Wisniewski
University of Central Florida
151 PUBLICATIONS **2,594** CITATIONS
SEE PROFILE

CO-oPS: A Mobile App for Community Oversight of Privacy and Security

Mamtaj Akter
Vanderbilt University
Nashville, Tennessee, USA
Mamtaj.Akter@vanderbilt.edu

Leena Alghamdi
University of Central Florida
Orlando, Florida, USA
Leenaalghamdi@knights.ucf.edu

Dylan Gillespie
University of Central Florida
Orlando, Florida, USA
Dgillespie00@knights.ucf.edu

Nazmus Sakib Miazi
Northeastern University
Boston, Massachusetts, USA
M.Miazi@northeastern.edu

Jess Kropczynski
University of Cincinnati
Cincinnati, OH, USA
Jess.Kropczynski@uc.edu

Heather Lipford
University of North Carolina, Charlotte
Charlotte, North Carolina, USA
Heather.Lipford@uncc.edu

Pamela J. Wisniewski
Vanderbilt University
Nashville, Tennessee, USA
Pamela.Wisniewski@vanderbilt.edu

ABSTRACT

Smartphone users install numerous mobile apps that require access to different information from their devices. Much of this information is very sensitive, and users often struggle to manage these accesses due to their lack of tech expertise and knowledge regarding mobile privacy. Thus, they often seek help from others to make decisions regarding their mobile privacy and security. We embedded these social processes in a mobile app titled "CO-oPS" ("Community Oversight for Privacy and Security"). CO-oPS allows trusted community members to review one another's apps installed and permissions granted to those apps. Community members can provide feedback to one another regarding their privacy behaviors. Users are also allowed to hide some of their mobile apps that they do not like others to see, ensuring their personal privacy.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Community Oversight; Mobile Privacy; Online Safety; Android phone; Mobile Apps; App Permissions

ACM Reference Format:
Mamtaj Akter, Leena Alghamdi, Dylan Gillespie, Nazmus Sakib Miazi, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2022. CO-oPS: A Mobile App for Community Oversight of Privacy and Security. In *Companion Computer Supported Cooperative Work and Social Computing (CSCW'22 Companion), November 08–22, 2022, Virtual Event, Taiwan.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3500868.3559706

CSCW'22 Companion, November 08–22, 2022, Virtual Event, Taiwan

ACM ISBN 978-1-4503-9190-0/22/11…$15.00
https://doi.org/10.1145/3500868.3559706

1 INTRODUCTION

85% of US citizens own smartphones [17] and 77% of them reported that they downloaded and installed mobile applications ("apps") on their smartphones [6]. These mobile apps often require access to users' sensitive information, like contact data, emails, location, calendars, and even browser history [1]. Although most of these apps request users' permission before accessing any information or resources, many apps secretly gathered users' system resources (e.g., camera, GPS) and private information (e.g., contacts list, text messages, emails) without users' consent [7, 19]. Therefore, most smartphone users are concerned about their mobile information privacy as they are not aware of how these mobile apps are using these resources [10]. This lack of transparency and users' lack of privacy and security knowledge cause them to seek advice and guidance from their close ones for making their digital privacy and security choices [11]. People also often learn about privacy and security from others in their social network, and this indirect learning eventually influences them to change their privacy behavior [12, 20].

Therefore, many researchers have acknowledged the importance of these social processes for managing individual, and collective digital privacy and security [9, 16, 18]. Some other recent studies proposed mechanisms that allowed trusted members of a community to help one another in making their digital privacy and security decisions [4, 8]. For example, Chouhan et al. proposed a mechanism titled Community Oversight for Privacy and Security ("CO-oPS") that allowed a group of trusted members of a community to help one another manage their mobile privacy and security, utilizing the concepts of individual participation, transparency, trust, and awareness. We converted this Community Oversight mechanism into a mobile app titled CO-oPS [8]. CO-oPS allows individuals to

review the apps installed and permissions granted on their community members' phones. It also lets users provide direct feedback to one another about their privacy and security behavior.

2 BACKGROUND

The proliferation of smartphone devices and the usage of mobile applications caused mobile phone users be over-exposed to the app permission requests and therefore they often overlook the permission prompts [21]. Mobile app users often do not fully understand what these mobile app permissions do and what are they used for and they do not even know where their data are being sent through accepting these permissions [5, 13, 14]. Recent privacy research [7, 19] also reported that many third party mobile apps automatically grant some permissions and accessed users' sensitive information which the users never explicitly acknowledged [19].

Due to the lack of privacy awareness and transparency among these app permissions, technology users often seek advice and guidance from their loved ones to make decisions regarding privacy and security [11, 15]. People also learn from their social network and eventually get influenced to change their privacy behavior [12, 20]. Hence, many network privacy researchers emphasized the importance of social collaboration [9, 16, 18] in managing privacy and security. With a goal to implement a technological solution to provide this social collaboration ability, we developed a novel mobile application titled CO-oPS (Community Oversight for Privacy and Security). The purpose of this app is to help mobile users mitigate their privacy awareness and knowledge gap by allowing them interact with their community and work together to keep their information safe from third party mobile apps. The next section discusses the overview and functionality of the features of our proposed mobile privacy app CO-oPS.

3 CO-OPS APP DESIGN

CO-oPS allows all community members to review the apps installed on one another's phones. It also allows checking what permissions are granted or denied to the installed apps. So, CO-oPS does not just let users monitor other community members' apps installed; it enables them to watch whether these apps access any sensitive data (e.g., contacts, emails, photos, location, browser history) from their phones. It also allows users to hide any of their own apps that they are not comfortable sharing with others, supporting their personal privacy. We developed this app based on the design suggestions made in our previous study by Chouhan et al [8]. They proposed a novel mechanism for users to interact with people they trust to help one another make digital privacy and security decisions regarding mobile app permissions. Their participatory design study provided some design suggestions to translate this framework into mobile app features. We leveraged those feature suggestions and implemented a full-functioning mobile app in this work. CO-oPS app includes six main features: 1) Community Apps, 2) Own Apps, 3) App Permissions, 4) Community Members, 5) Individual Apps, and 6) Community Feed.

- *Community Apps (Figure-1):* Under the Discovery tab, the All Apps section presents the list of all apps that are installed on all community members' phones. The icon and name of the app is displayed, along with the word "Installed" if the user has that app

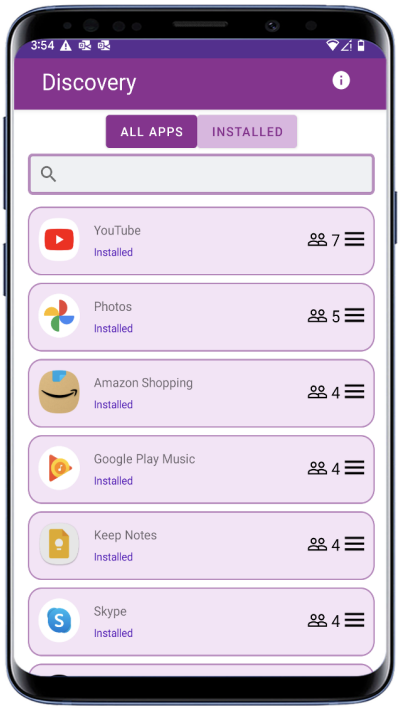

Figure 1: Community Apps

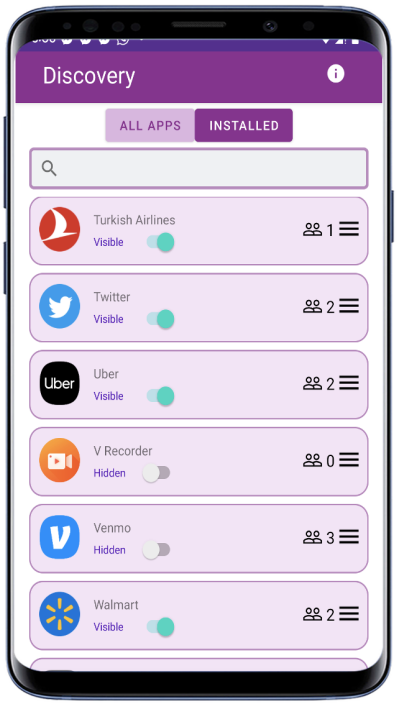

Figure 2: Own Apps

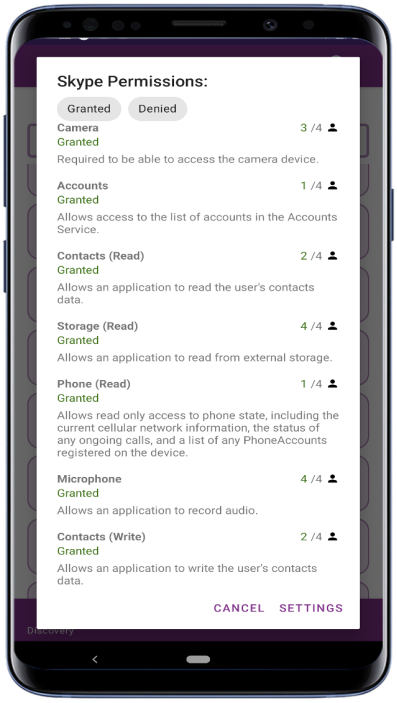

Figure 3: App Permissions

Figure 4: Community Members

on their phone. On the right side of the screen is a number indicating how many members of the community have the app installed, along with a three line menu icon that will open an app permissions dialogue box. The All Apps section can be used to find apps that others in the community are using and find potentially concerning apps that a user may want to discuss with the other members.

- *Own Apps (Figure-2):* The Installed section displays only apps that the user has installed on their own device. Alongside the icon and name of each app is a switch that allows users to toggle the visibility of each app between "Visible" and "Hidden". Apps on your device that are changed to hidden will not be viewable to other members of the community. Information shown on the right side of the screen for each app is the same as in the All Apps section.

- *App Permissions (Figure-3):* The App Permissions section appears as a dialogue box and shows how many community members have granted or denied a permission for a specific app. For each permission an app requests there will be a description of what it accesses and a readout of how many community members out of the total number have granted or denied a permission. If members of the community have granted the permission the word "Granted" will be displayed in green text. If they have denied the permission the word "Denied" will be displayed in red text. The permissions can be filtered by Granted or Denied by tapping the labeled buttons at the top of the screen. This section can also bring users directly to their phones app permissions settings menu by tapping the settings button at the bottom of the page. This section can be used to compare what permissions the user has granted with their community and see if they are in consensus about what permissions to grant to certain apps. If they are not this may lead to a discussion on what permissions ought to be granted.

- *Community Members (Figure-4):* Information relating a specific community member can be found within the People tab. Here a profile picture for each community member is displayed along with "messages" and "explore" buttons. The messages button next to each community members will take users to a page where they can message that specific member to discuss privacy issues or give feedback about suspicious apps or app permissions. The explore button allows users to view the apps that a specific community member has installed.

- *Individual Apps (Figure-5):* Within the Explore section a user can see the apps installed on an individual community member's device. This section is laid out like the All Apps section on the discovery page except it only lists apps that the selected community member has installed. Tapping the three line menu icon will take the user to the app permissions page for that app. The explore feature could be used to locate a suspicious app that a community member have installed so that the user to could then message that specific community member to provide guidance about their apps.

- *Community Feed (Figure-6):* The community feed functions like a forum where community members can make posts and others can like those posts and reply to them. This feed can be used to initiate discussion with all other community members about specific apps, permissions or any general strategies to keep the community safe. The community feed also provides weekly pro-tips from the CO-oPS app to help community members remain aware with regards to privacy, security installing new apps, and granting permissions.

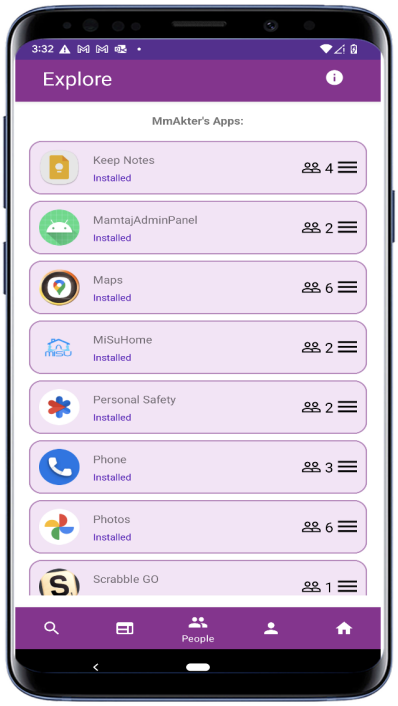

Figure 5: Individual's Apps

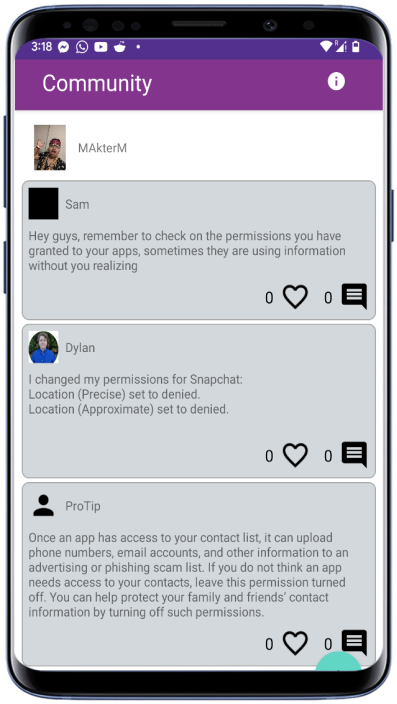

Figure 6: Community Feed

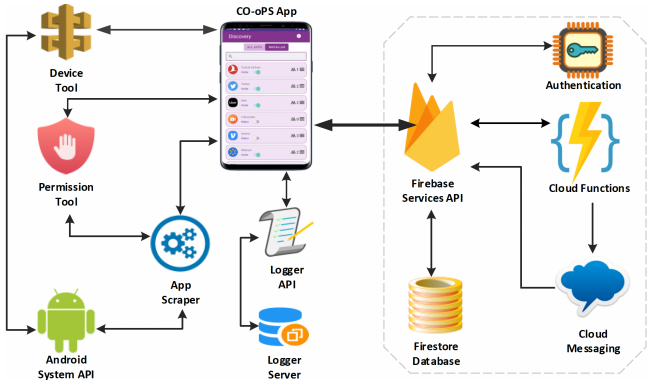

Figure 7: CO-oPS System Architecture

4 SYSTEM ARCHITECTURE

The CO-oPS app is developed with an Android native front-end and a hybrid back-end consisting of Firebase cloud services and NodeJS servers. It uses three main back-end APIs (Figure-7) for its user interactions: 1) AppScraper, 2) DeviceTool, and 3) PermissionTool. AppScraper is a utility designed to execute background threads to access local on-device data using Android systems API. This tool collects app metadata on the device, compares it against the remote catalog of apps, and sends any relevant changes to Firebase. Through the DeviceTool API, the device ID, SIM serial number, and Android ID are fetched. The PermissionTool API serves to convey the permissions associated with a given app. In addition to these three, the CO-oPS app uses a custom-built authentication API that employs Firebase and DeviceTool API to fit the unique need to form CO-oPS groups. Also, the app uses an API with a NodeJS back-end to store the anonymized logs of the app usage. Lastly, this app consists of a push notification API managed by Firebase Cloud Functions to maintain a seamless and effective group interaction.

5 LIMITATIONS AND FUTURE WORK

While the CO-oPS app provides many important benefits, e.,g., a collaborative platform to co-manage mobile privacy, and personal privacy by hiding apps, it still has some drawbacks that we intend to mitigate in the future. One of the most significant limitations of this app is it does not provide any suggestions or recommendations regarding the app permissions. When users are less tech-savvy or have less knowledge and awareness about mobile app permissions, they might not know which permissions are safe or dangerous. Although this app currently provides weekly pro tips to educate users, in a future version of this app, we intend to implement push notifications to alert the users when any of their apps acquire dangerous permissions (e.g., account, location, contacts). Additionally, CO-oPS app falls short in usability. The user might want to review their apps by the permission names. For example, they might want to view the group of apps that have a specific permissions granted. For example, a user may want to view the list of their apps that have the precise location permission granted. The primary purpose of this app is to help communities in securing their information from third-party apps, and so it is crucial to redesign this app such that users can view and group their apps by the permissions granted.

Additionally this app may not be applicable among families with hierarchical tensions (e.g., parents and teens) as it allows privacy in their app usage and equal power in co-monitoring [3]. Future iterations of this app need to consider such cases to allow family members to help one another manage their mobile privacy. We also can examine whether this app can help parents and teens be influenced by one another's app usage and permission decisions to change their online safety [2] and privacy behaviors. Lastly, we intend to launch a longitudinal field study where groups of people (friends, families, communities) can try different features of this app and give their feedback on a weekly basis.

6 CONCLUSION

Our CO-oPS app represents a shift from an individual's effort to a collaborative relationship in managing mobile privacy and security. By including the loved ones in CO-oPS network, individuals who are less knowledgeable about mobile privacy can receive oversight from those who have more knowledge. This app also has the potential to initiate open discussions regarding the app permission issues. From an older adults to a teen in families, CO-oPS can benefit a wide range of age groups and provide an interactive solution to keep everyone safe online and secure sensitive information.

ACKNOWLEDGMENTS

We acknowledge the contributions of Nicholas Osaka, Anoosh Hari and Ricardo Mangandi, who developed the CO-oPS application. This research was supported by the U.S. National Science Foundation under grants CNS-1844881, CNS-1814068, CNS-1814110, and CNS-1814439. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

[1] 2015. Mobile apps, privacy and permissions: 5 key takeaways. https://www.pewresearch.org/fact-tank/2015/11/10/key-takeaways-mobile-apps/

[2] Zainab Agha, Reza Ghaiumy Anaraky, Karla Badillo-Urquiola, Bridget McHugh, and Pamela Wisniewski. 2021. 'Just-in-Time' Parenting: A Two-Month Examination of the Bi-directional Influences Between Parental Mediation and Adolescent Online Risk Exposure. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Springer International Publishing, Cham, 261–280.

[3] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1, Article 57 (apr 2022), 28 pages. https://doi.org/10.1145/3512904

[4] Zaina Aljallad, Wentao Guo, Chhaya Chouhan, Christy LaPerriere, Jess Kropczynski, Pamela Wisnewski, and Heather Lipford. 2019. Designing a Mobile Application to Support Social Processes for Privacy (Journal Article) | DOE PAGES. https://par.nsf.gov/biblio/10097722

[5] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J. Wisniewski. 2022. Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 406, 18 pages. https://doi.org/10.1145/3491102.3517652

[6] Michelle Atkinson. 2015. Majority of U.S. Smartphone Owners Download Apps. https://www.pewresearch.org/internet/2015/11/10/the-majority-of-smartphone-owners-download-apps/

[7] Paolo Calciati, Konstantin Kuznetsov, Alessandra Gorla, and Andreas Zeller. 2020. Automatically Granted Permissions in Android apps: An Empirical Study on their Prevalence and on the Potential Threats for Privacy. In *Proceedings of the 17th International Conference on Mining Software Repositories (MSR '20)*. Association for Computing Machinery, New York, NY, USA, 114–124. https://doi.org/10.1145/3379597.3387469

[8] Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2019. Co-designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–31. https://doi.org/10.1145/3359248

[9] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, 143–157.

[10] Fred Davis and Fred Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *" "* 13 (1989), 319. https://doi.org/10.2307/249008

[11] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (Nov. 2004), 391–401. https://doi.org/10.1007/s00779-004-0308-5

[12] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/2335356.2335360

[13] Denzil Ferreira, Vassilis Kostakos, Alastair R. Beresford, Janne Lindqvist, and Anind K. Dey. 2015. Securacy: an empirical investigation of Android applications' network usage, privacy and security. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/2766498.2766506

[14] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J. Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 686, 14 pages. https://doi.org/10.1145/3411764.3445204

[15] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. 2021. Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 396 (oct 2021), 23 pages. https://doi.org/10.1145/3479540

[16] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors | Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. https://dl.acm.org/doi/10.1145/2998181.2998323

[17] 1615 L. St NW, Suite 800 Washington, and DC 20036 USA202-419-4300 | Main202-857-8562 | Fax202-419-4372 | Media Inquiries. 2021. Demographics of Mobile Device Ownership and Adoption in the United States. https://www.pewresearch.org/internet/fact-sheet/mobile/

[18] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (Sept. 2015), 121–144. https://doi.org/10.1093/cybsec/tyv008 Publisher: Oxford Academic.

[19] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *WINTER 2019, VOL. 44, NO. 4* (2019). USENIX, Boston, MA, United States, 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[20] Stuart Schechter and Joseph Bonneau. 2015. Learning Assigned Secrets for Unlocking Mobile Devices. In *" "* (2015). USENIX, " ", 277–295. https://www.usenix.org/conference/soups2015/proceedings/presentation/schechter

[21] Sarina Till and Melissa Densmore. 2019. A Characterization of Digital Native Approaches To Mobile Privacy and Security. In *Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019 (SAICSIT '19)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3351108.3351131