It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-based Privacy and Security for Mobile Smartphones

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

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

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

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

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

ABSTRACT

We conducted a user study with 19 parent-teen dyads to understand the perceived benefits and drawbacks of using a mobile app that allows them to co-manage mobile privacy, safety, and security within their families. While the primary goal of the study was to understand the use case as it pertained to parents and teens, an emerging finding from our study was that participants found value in extending app use to other family members (siblings, cousins, and grandparents). Participants felt that it would help bring the necessary expertise into their immediate family network and help protect the older adults and children of the family from privacy and security risks. However, participants expressed that co-monitoring by extended family members might cause tensions in their families, creating interpersonal conflicts. To alleviate these concerns, participants suggested more control over the privacy features to facilitate sharing their installed apps with only trusted family members.

CCS CONCEPTS

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

KEYWORDS

Community Oversight; Collaborative Approach; Joint Oversight; Family Online Safety; Mobile Privacy; Digital Privacy; Security

ACM Reference Format:
Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2023. It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-based Privacy and Security for Mobile Smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3544549.3585904

CHI EA '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3585904

1 INTRODUCTION

A Pew Research study reported that 85% of U.S. citizens own smartphones [21], and 77% of them have downloaded and installed different third-party mobile apps on their devices [6]. Mobile apps collect personal information (e.g., contact data, emails, photos, location, calendar events, and even browser history) from users when granted permission to do so [5], creating digital privacy threats when this personal information is misused [9, 25]. Unfortunately, the majority of U.S. adults lack knowledge regarding how to protect their digital privacy and security, which increases the potential for privacy and security violations [28]. Due to the lack of mobile privacy knowledge at an individual level, networked privacy researchers (e.g., [3, 10, 13]) have suggested adopting more collaborative and community-based approaches for managing digital privacy and security, where trusted community members (e.g., family, friends, co-workers) can work together to help keep one another safe online. Interestingly, some research has even shown how adult family members often rely on younger generations of their family (e.g., their teens) for technology support, as youth may be tech-savvier than their parents [11, 27].

For instance, a recent study [2] examined family online safety and privacy management by asking parents and teens to evaluate a collaborative mobile app to understand whether parents and teens can help one another manage their mobile privacy and online safety. Despite the hierarchical tensions and asymmetry in privacy and security knowledge between the parents and teens, they found value in such bi-directional joint family oversight for keeping both parties safer online. Meanwhile, our current work acknowledges that a family often consists of other relationships beyond just parents and teens; therefore, it is unclear whether this collaborative approach could be generalized for the whole family by going beyond the parent-teen dyadic relationship. As such, we build upon prior work with parents and teens and extend it by exploring whether, how, and why joint family oversight that includes extended family members may work given a similar use case. Therefore, we first developed a mobile app for Community Oversight of Privacy and Security ("COoPS"). Second, we had 19 parents and teens install and evaluate the app in a lab-based setting. In addition to understanding the dynamics of using the app within the context of the parent-teen

relationship, participants also expressed the value of including additional family members within the app for broader oversight within an extended family network. As such, we were able to answer the following high-level research questions:

- **RQ1:** *With whom else could they see including in their trusted networks when sharing and receiving advice on mobile privacy and security?*
- **RQ2:** *What would be the potential benefits and drawbacks of including extended family members in a joint family approach?*
- **RQ3:** *What are the important design considerations for designing an app for joint family oversight that includes extended family members?*

Overall, parents and teens felt that they would use the CO-oPS app with their close relatives, particularly grandparents, siblings, and cousins (RQ1). Parents and teens both saw benefits in co-managing their mobile privacy and online safety with their extended families as they thought it would help benefit more vulnerable family members (the older adults and children), and get more expert advice from others within the family who are tech-savvier. However, having extended families included in the CO-oPS family network might also cause unwanted tension and interpersonal issues for the parents and teens, e.g., blaming parents for teens' mobile online behavior, disallowing teens' autonomy, unwanted questioning, and family arguments (RQ2). To alleviate these concerns, they suggested implementing more controls within the privacy feature so that they can share their installed apps with only specified family members (RQ3). Our research makes important contributions to the networked privacy research community by examining whether co-managing mobile privacy, online safety, and security with other family members, beyond just the parent-teen relationship, could potentially help keep entire families safe online.

2 BACKGROUND

We place our study within two main streams of research: 1) mobile privacy and security management on the individual level, and 2) collaborative approaches for mobile privacy, safety, and security.

2.1 Mobile Privacy and Security Management at the Individual Level

The proliferation of the usage of smartphones and mobile applications [21] caused mobile phone users to be over-exposed to digital privacy, safety, and security threats [5, 28], as mobile apps get access to users' sensitive and personal information via different permissions [5, 28]. Ironically, mobile app users often do not fully understand what these mobile app permissions do and what they are used for [4, 15, 16, 22]. Users also lack the understanding of how their personal data are being used by these third parties [16]. What is worse, third-party mobile apps may even get unauthorized access to users' information [9, 25]. For example, Calciati et al. [9] found that when users give single permission, the app can silently obtain further permissions. They further revealed that many third-party apps leaked and misused users' sensitive data, such as the user's precise location, list of contacts, history of phone calls, and emails, the permissions which users never explicitly granted. Despite these various privacy threats, the majority of US adults lack significant knowledge regarding digital privacy and security and therefore, find it difficult to manage their own privacy and security [28]. In the next section, we synthesize the relevant literature that suggests adopting collaborative approaches to help resolve individual's challenges in privacy and security management.

2.2 Collaborative Approaches for Mobile Privacy, Safety, and Security

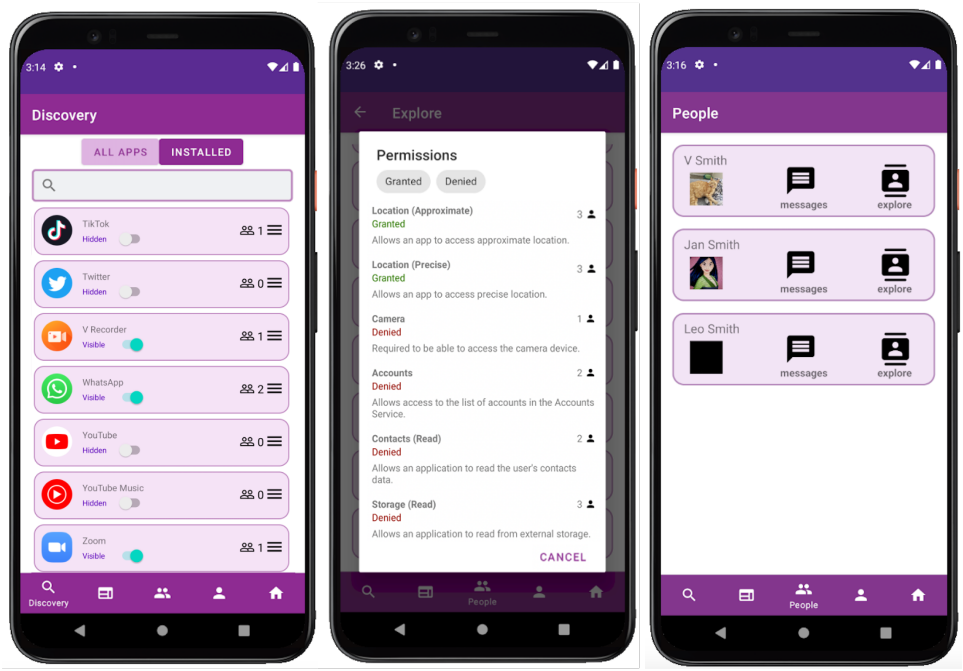
Several networked privacy research studies have demonstrated that individuals often seek help and informal advice from their trusted community (e.g., families, friends, coworkers) regarding digital privacy and security [23, 24]. Users are also influenced by others' privacy and security practices to make changes to their own privacy behaviors [12–14, 17, 26]. Therefore, networked privacy researchers have called for more collaborative approaches within an individual's networks so that people can exchange mobile privacy, safety, and security support with one another [3, 10, 13].

However, Kropczynski et al. [19] have reported that in order to get effective support for digital privacy and security management, one must have some technical expertise in their community. Meanwhile, studies have indicated that teens often provide informal tech support to their family members [11, 18]. In a recent study, Akter et al. [2] examined a collaborative family oversight approach that allowed teens and their parents to help one another manage their mobile online safety and privacy. Their lab-based study revealed that parents and teens overall valued such collaborative approaches to manage their online safety and mobile privacy. However, there were some tensions between parents and teens because of the differences in hierarchical power and tech-savviness. This work gave us the idea to further investigate whether such joint family oversight mechanisms would be applicable to the other relationships in the family. Building upon these prior studies, we explore whether an app created for Community Oversight of Privacy and Security ("CO-oPS") [10] could be beneficial for immediate and extended families to work together to help one another manage their mobile online safety, privacy, and security.

3 METHODS

3.1 Design of the CO-oPS App

We developed the CO-oPS app [1] based on the model of community oversight for privacy and security initially proposed by Chouhan et al. in [10]. This model suggests mechanisms for trusted communities to review one another's mobile privacy and security practices (apps installed and permissions granted) and exchange guidance. The CO-oPS app includes three key aspects: 1) discovery of installed apps, 2) permissions granted/denied, and 3) people in the family. The Discovery feature (Figure-1a) allows users to review the list of installed apps on their own phone with the ability to hide some apps from their family members. The permissions feature (Figure-1b) allows users to review the permissions granted or denied to each of the apps installed. In the People screen (Figure-1c), users can view the list of their family members with the ability to directly message them and explore their installed apps. Here, to help the parents and teens imagine using this app with their other family members, we added two fictional family members: the teen's uncle and aunt.



(a) (b) (c)

Figure 1: CO-oPS features: (a) Discovery of Installed Apps, (b) Permissions Granted/Denied, (c) People in the Family

Therefore, during the study, each participant viewed three people in this family list.

3.2 CO-oPS Parent-Teen User Study

Our study consisted of two distinct phases: 1) A guided think-aloud exploration of the CO-oPS app with probing questions, and 2) A semi-structured interview with parents and teens, with one component where we asked them to reflect on whether using this with the other family members (including extended family) would be useful for them. The study session started with showing participants a video demo of the CO-oPS app to explain its core functionalities. The participants were then asked to install the app on their phones and use its different features, as shown in Figure-1. We asked probing questions to learn about participants' reactions to the fictional family members presented on the CO-oPS People page, as well as their suggestions as to who else they would prefer to have in their CO-oPS family network. The presentation of these two extended family members motivated our participants to think about the potential benefits of allowing their extended family to participate in their joint family oversight and encouraged them to think about their concerns of having these family members included in reviewing their apps' permissions. Thus, participants could consider both benefits and drawbacks, which also helped them to brainstorm design suggestions that can support the benefits and alleviate the drawbacks of having extended family included in the CO-oPS family network.

The study sessions took place on Zoom and were audio and video recorded. We then transcribed the recordings and conducted a grounded thematic analysis for insights, using Braun & Clarke's [8] six-phase framework. Overall, we recruited a diverse sample of 19 parent and teen pairs where 42% of the participants were Asian, 32% Caucasian, 21% Hispanic / Latino, and 5% African American families. 53% of the teens self-reported as females, and 47% were males, whereas 58% of the parents were female, and 43% were male. The teens' ages ranged from 13-17, with a mean age and standard deviation of 15.4 and 1.4, respectively. The parents' mean age and the standard deviation were 47.7 and 4.76, respectively, where their ages ranged between 40 to 55.

4 RESULTS

In this section, we present the themes that emerged from our qualitative analysis regarding the inclusion of extended family in CO-oPS. Participants' quotations are identified by their IDs (for teens: T1, T2,..T19 and parents: P1, P2,..P19), age, and gender information.

4.1 People to whom the joint family approach could be extended (RQ1)

Most of the parents and teens felt that they would extend the joint family oversight approach to their grandparents, siblings, and cousins. More than two-thirds of the parents (68%, N=13) and half of the teens (53%, N=10) said they would be interested to have their **parents (teens' grandparents)** in their CO-oPS family network since they are the closest ones in their family who provide them support, care, and acceptance.

> *"This would be very useful if you include your grandparents. They'd probably freak out if they knew all the apps that are sharing their location...they can then rely on us to help them with the permissions... It's not just they are family, they care about us, they love our kids."* – P9, Female, 51 years old

Teens showed more flexibility in terms of including other family members, such as siblings, and cousins. About half of the teens (58%, N=11) and a few parents (16%, N=3) said they would like to include their **siblings and cousins (parents' other children, nephews and nieces)** into their CO-oPS family network. We noticed that teens showed more enthusiasm in co-managing with their siblings and cousins because they are of similar age and they get along with them easily. A good number of parents (42%, N=8) also said they would like to include their own **siblings (teen's uncles and aunts)** as they are close to their immediate family. Interestingly, around one-third of the parents (32%, N=6) mentioned they would monitor their **significant other's** mobile apps and permissions as they are not much aware of the importance of using safe apps and granting safe permissions.

4.2 Potential benefits and drawbacks of including extended family (RQ2)

Parents and teens, in general, envisioned benefits in the joint family oversight with their other family members but also saw some potential concerns for including extended family who are not as close to them.

Most parents and teens thought such joint family oversight would be beneficial for the vulnerable people of their families. More than half of the participants (63%, N=12 parents and 47%, N=9 teens) mentioned that the CO-oPS app would **help the older adults**, as they often are less aware of the digital privacy threats and also lack the knowledge to monitor or manage app permissions. Both the parents and teens thought that through the CO-oPS app, they would be able to help the older adult family members by letting them know about their unsafe apps and permissions. Next, 58%, N=11 teens felt it would **benefit younger children** as they also tend to be less aware of mobile privacy and security issues, similar to the older adults.

> *"A lot of older people like my parents, or like the old people in general, they do not get much time, they are not very tech-savvy either... If my parents, they're included in our app like that,...it would help them."* – P8, Female, 46 years old

Parents and teens also saw value in including extended families in the joint family oversight as it would bring necessary expertise into their family network. Almost half of the teens (47%, N=9) and a couple parents (11%, N=2) mentioned that they would be able to **get more expert advice or guidance from the tech-savvy people** of the extended family. Here, teens mostly mentioned their tech-savvy older cousins and siblings. Similarly, N=2 parents also mentioned their tech-savvy siblings who have better knowledge regarding mobile privacy and security. Apart from this, around one-fourth of the participants (21%, N=4 parents and 26%, N=5 teens) said that having their extended family would help them more in terms of being safe online and securing their personal information as more people would be able to **warn them about unsafe apps**. To this end, they often referred to some popular but controversial social media and gaming apps, e.g., TikTok, Snapchat, Discord, and Instagram, that they came to know from their extended family members. Hence, having more family members in the CO-oPS family network would help them be more aware of different mobile apps and their privacy issues.

> *"This would be more about educating the mind and creating awareness because they're [cousins] gonna reevaluate your apps. So we might as well all learn from each other."* - T14, Female, 16 years old

Parents saw additional benefits in including extended family as they would get more help in monitoring their children's mobile online safety. Around half of the parents (47%, N=9) felt that involving extended family, especially their siblings (teens' uncles and aunts), in the CO-oPS family network would enable them to **share the parental responsibilities** to monitor teens' app usage. These parents thought that their siblings would care about their teens as much as they did, and so, they would have some peace of mind knowing there would be other people to monitor their children's mobile online safety. Additionally, one-third of the parents (32%, N=6) said their children would consider listening to the advice more when they would receive **guidance and feedback from more people**. A few parents (26%, N=5) also thought using CO-oPS with extended family would **strengthen the relationship** between their children and the other family members who live out of their town or state as they would get an opportunity to work together on managing their family online safety and privacy.

> *"Our extended family is pretty concerned about this stuff. So, this is a lot easier to kind of check on our kids, you know to make sure they are not using anything dangerous, and I would know that there are others to tell them about if any safety concerns they might have."* - P2, Female, 50 years old

Participants felt that including their extended family in the joint family oversight would bring more tensions. Almost half of the parents (47%, N=9) and one-fourth of the teens (26%, N=5) expressed that involving the extended family in co-managing their mobile privacy and security might become **more stressful for parents**. They felt that the extended family might blame parents for teens' unsafe online safety behaviors, especially if they find inappropriate mobile apps on teens' phones. Interestingly, 43%, N=8 teens said such co-managing mobile privacy and security would cause more harm for them because parents might get provoked to **pull away their autonomy** in using social media, the internet, or even mobile phones. They often brought up the restrictive and authoritarian parenting styles in their uncles' and aunts' families, where their cousins are not allowed to own mobile phones, and this might influence their parents to adopt such restrictions in their family as well. A few participants (16%, N=3 parents and 5%, N=1 teens) specifically said that they **did not see any necessity** of including their extended family as they are not close.

> *"I think once it reaches like extended families, like grandparents and aunts and uncles, it could get a little bit harmful because these are people you aren't living with or aren't as close. I think mostly there would be just*

> *drama with my parents, oh, they're doing this or that, you know, stressing them more."* - T13, Female, 13 years old

Participants also expressed concerns for potential interpersonal conflicts that might arise. More than one-third of the participants (N=42%, N=8 parents and N=32%, N=6 teens) envisioned that some people in the extended family might become officious and therefore, there will be some **unnecessary questioning about their personal choice of app usage**. Some participants (N=37%, N=7 parents and N=21%, N=4 teens) also believed that there would be more incidence of **family arguments when either parents or teens ignore the advice given** regarding their mobile apps installed or permissions granted.

> *"But if it's for the apps, and then you'll hear like why do you have this app for, then I don't think you have the right to do it [questioning] because they're not completely as close as my immediate family. It's like giving them a new scope to roast me for using a particular app."* -T16, Female, 14 years old

4.3 Design suggestions for a joint family oversight app (RQ3)

Participants suggested more control over the app privacy features to allow only specific people to co-monitor their apps and permissions. Around half of the parents (47%, N=7) and one-fourth of the teens (26%, N=5) mentioned that they would want to keep their apps visible only to their immediate families and **to some specific people** of their extended families, due to the drawbacks highlight above. A couple of teens (11%, N=2) also said they would want the ability to **hide from their dominating older siblings**. Interestingly, about one-third of the parents (32%, N=6) mentioned that they would like to **hide their teens' apps** from their extended family to avoid any potential tensions or conflicts from happening. Parents often said that they would either manually take their teens' phones or ask their teens to hide their installed apps from the extended family.

> *"If this went beyond my immediate family, my husband, and kids, then I would probably reconsider that thought. I would not want all of them to check my things, I would hide apps from them... But again, if there is any option to keep it shown for just a few people from the extended family, not all of them, that would be nice."* – P12, Female, 55 years old

Additionally, a few parents (16%, N=3) and teens (21%, N=4) suggested additional features that would allow them to **remotely change the apps and permissions** on their extended family members' phones. These participants mostly wanted such features to help some of their relatives who are non-tech savvy and do not live with them. To further explain, they often said that being able to review and let them know would not be enough actually to help them. As some of their extended family, e.g., grandparents, do not have any technical knowledge, they would not be able to follow others' feedback and go to the settings to deny permissions. Therefore, these parents and teens expressed that they would like to have the ability to remotely change the apps and permissions on their family members' phones.

> *"If we could use that with like my grandparents, I would want to change from here [CO-oPS], because they may not know how to go into the place and they can't change it. If you're able to do it here. That would be a thing like I needed in our situation."* - T3, Female, 14 years old

5 DISCUSSION

One of the key lessons learned was that our participants did not implicitly envision their whole family as their CO-oPS family network. They instead envisioned using this family oversight app with people in the family who have strong bonds with them. This reconfirms one of the findings of Chouhan et al.'s paper [10], where their participants were primarily motivated to help only close people. Also, while opening the CO-oPS family network to others in the extended family, our participants were also keenly aware of the trade-off between getting more help versus being able to avoid potential arguments and interpersonal conflicts. As a result, participants tried to negotiate this tension by filtering out the visibility of their apps based on whether someone was close to them or not. Therefore, a key takeaway of our work is to make sure the family members have full agency over with whom their apps are being shared. This desire for more controls is in contrast with the results from Akter et al. [2], where participants saw little use of privacy features within just the parent-teen context [2].

On the other hand, our participants wanted to include their extended family in the joint family oversight not only to receive expert advice from others, but also to provide help as well [7]. For instance, parents and teens were willing to include tech-savvy family members in their CO-oPS family network who can help them with privacy and security advice and guidance. This was because they felt the needed expertise that did not exist within their immediate family. In Akter et al.'s work [2], they found that teens did not trust the feedback of their parents, as they perceived their parents as less tech-savvy. Therefore, including the extended family might provide them with the dependable expert advice and guidance that teens need. Our participants also showed equal enthusiasm to provide help to other family members, especially to older adults who are less tech-savvy. In Kropczynski et al.'s studies [19, 20], they found that older adults tend to be on the receiving end of tech support [27], whereas younger adults are more likely to be tech support givers. So, joint family oversight could support such tech caregiving mechanisms, including the support for mobile privacy and security. Akter et al. [2] reported in their study that teens did not feel empowered to monitor their parents' apps and permissions and hence, were reluctant to participate in joint family oversight. So, teens' being interested to provide help to others in the extended family, such as their grandparents, shows the potential for increasing their engagement in the joint family oversight mechanism.

6 LIMITATIONS AND FUTURE RESEARCH

We recognize several limitations of our study. First, we examined the perceived benefits and drawbacks of using the CO-oPS app with extended family members only from the parents' and teens' perspectives, as this was an emergent finding from our primary study that was worthy of further investigation. As such, it would be an important next step to explore extended family members'

opinions in future work. Another potential limitation was that we presented the teens' uncle and aunt as their fictional extended family members on CO-oPS, which might have led participants to think more about the prospective problems that might arise from co-managing with these family members. Interestingly, however, our participants felt that they would use the CO-oPS app mostly with their other relatives: teens' grandparents, siblings, and cousins. Lastly, because the nature of our study was lab-based, parents and teens could not evaluate the CO-oPS app in a realistic setting; thus, in future studies, we would want to deploy the CO-oPS app among groups of family members, including diverse family relationships.

7 CONCLUSION

Given the continued proliferation and usage of smartphones and third-party mobile apps, we believe community members can work side by side to co-manage their mobile privacy, safety, and security. Our study explored a joint family approach, highlighting parents' and teens' perceived benefits, concerns, and design considerations for co-managing their mobile privacy and security with other members of their extended families. Our work demonstrates the added benefits and challenges when broadening an oversight community beyond parents and teens. Generally, participants felt that such a collaborative approach with extended family would help them exchange privacy and security support with those they cared about. Yet, potential tensions and interpersonal conflicts would require additional controls on collaborative monitoring so that only trusted and close family members can review their mobile privacy and security behaviors. We will continue to build upon this work to examine how we can help people successfully co-manage mobile privacy, safety, and security within their families.

ACKNOWLEDGMENTS

We acknowledge the contributions of Nazmus Sakib Miazi, Nikko Osaka, Anoosh Hari, and Ricardo Mangandi in developing the CO-oPS application. We would also like to thank the parents and teens who participated in our study. This research was supported by the U.S. National Science Foundation under grants CNS-1844881, CNS-1814068, CNS-1814110, and CNS-1814439. Any opinions, findings, 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] 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 Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, Taiwan) *(CSCW'22 Companion)*. Association for Computing Machinery, New York, NY, USA, 179–183. https://doi.org/10.1145/3500868.3559706

[2] 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

[3] 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

[4] 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

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

[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] Karla Badillo-Urquiola, Zainab Agha, Mamtaj Akter, and Pamela Wisniewski. 2020. Towards Assets-based Approaches for Adolescent Online Safety. In *Badillo-Urquiola, Agha, Z., Akter, K., Wisniewski, P.,(2020)"Towards Assets-Based Approaches for Adolescent Online Safety" Extended Abstract presented at the ACM Conference on Computer-Supported Cooperative Work Workshop on Operationalizing an Assets-Based Design of Technology,(CSCW 2020)*.

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[9] 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

[10] 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

[11] Teresa Correa, Joseph Straubhaar, Wenhong Chen, and Jeremiah Spence. 2015. Brokering new technologies: The role of children in their parents' usage of the internet - Teresa Correa, Joseph D Straubhaar, Wenhong Chen, Jeremiah Spence, 2015. https://journals.sagepub.com/doi/10.1177/1461444813506975

[12] 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.

[13] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, Vancouver, BC, Canada, 1416–1426. https://doi.org/10.1145/2675133.2675225

[14] 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

[15] 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

[16] 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

[17] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[18] Sara Kiesler, Bozena Zdaniuk, Vicki Lundmark, and Robert Kraut. 2000. Troubles With the Internet: The Dynamics of Help at Home. *Human–Computer Interaction* 15, 4 (Dec. 2000), 323–351. https://doi.org/10.1207/S15327051HCI1504_2

[19] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 255:1–255:27. https://doi.org/10.1145/3432954

[20] 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

[21] 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/

[22] Jinkyung Park, Eiman Ahmed, Hafiz Asif, Jaideep Vaidya, and Vivek Singh. 2022. Privacy Attitudes and COVID Symptom Tracking Apps: Understanding Active Boundary Management by Users. In *Information for a Better World: Shaping the Global Future*, Malte Smits (Ed.). Springer International Publishing, Cham, 332–346.

[23] 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.

[24] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. Association for Computing Machinery, Washington, D.C., 1–17. https://doi.org/10.1145/2335356.2335364

[25] 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. 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[26] 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

[27] Bill Van Parys. 2019. You don't need to be tech savvy to be a tech caregiver. https://www.fastcompany.com/90438110/you-dont-need-to-be-tech-savvy-to-be-a-tech-caregiver

[28] Emily A. Vogels and Monica Anderson. 2019. Americans and Digital Knowledge. *Pew Research* (Oct. 2019). https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/