Designing a Mobile Application to Support Social Processes for Privacy Decisions

Zaina Aljallad
University of Central Florida
zaina.aljallad@knights.ucf.edu

Wentao Guo
Pomona College
wgtc2015@mymail.pomona.edu

Chhaya Chouhan
University of Central Florida
chhayachouhan@knights.ucf.edu

Christy LaPerriere
University of Central Florida
christylaperriere@knights.ucf.edu

Jess Kropczynski
University of Cincinnati
jess.kropczynski@uc.edu

Pamela Wisnewski
University of Central Florida
pamela.wisniewski@ucf.edu

Heather Lipford
University of North Carolina
richter@uncc.edu

***Abstract*–People often rely on their friends, family, and other loved ones to help them make decisions about digital privacy and security. However, these social processes are rarely supported by technology. To address this gap, we developed an Android-based mobile application ("app") prototype which helps individuals collaborate with people they know to make informed decisions about their app privacy permissions. To evaluate our design, we conducted an interview study with 10 college students while they interacted with our prototype. Overall, participants responded positively to the novel idea of using social collaboration as a means for making better privacy decisions. Yet, we also found that users are less inclined to help others and may be only willing to partake in conversations that directly affect themselves. We discuss the potential for embedding social processes in the design of systems that support privacy decision-making, as well as some of the challenges of this approach.**

I. INTRODUCTION

Within the last fifteen years, developments in digital technology have significantly changed our lives in many ways. For instance, personal information has never been as exposed and accessible as it is today [1], and this trend is expected to continue as new technologies make the collection of data even more feasible [2]. For instance, the political data firm Cambridge Analytica recently obtained the personal information of over 50 million Facebook users and used it for political purposes in the 2016 U.S. presidential election. Fewer than 300,000 of these individuals had given explicit consent to the collection of their data [3]. As technology continues to develop at a historically unprecedented pace, an increasing number of people are unable to keep up with its new features and demands. Smartphones, which are both widely used and vulnerable to information breaches, form a growing domain for privacy and security threats [4], [5]. In particular, significant amounts of personal information are being shared with third parties through apps [6]. App permissions, which provide smartphone users with control over what information is shared with apps, are often difficult to understand and lack transparency [7]. Users are often left unaware of significant privacy threats or choose to ignore them due to their incomprehensibility. Hence, more research is needed to examine mechanisms that can aid users in making more informed privacy decisions when using smartphones.

We explore social collaboration as a means for helping people make privacy decisions in the specific context of mobile smart phone app permissions. When people are in new situations or face uncertainty, they often ask trusted individuals for advice and model behaviors of their friends and/or loved ones [8]. These interactions can be reciprocal; the same individuals are also being observed or asked for advice by others. For instance, Aarstad et al.'s research on organizational learning found that employees often provide guidance to trusted colleagues [8]. Similarly, others found that individuals often work together within their social network of friends, family members, and coworkers to resolve privacy issues [9], [10]. Social influence exerted by trusted individuals has a significant impact on behavior [11].

Yet, when users make privacy decisions, these social processes are often not reflected in the design of networked technologies that could put them at risk for unintended privacy breaches. For example, when smartphone users decide which permissions to allow or deny when installing and using mobile apps, this process is very individualistic and misses the opportunity to facilitate social processes that support privacy decision-making. To address this gap, we designed a novel prototype for a mobile app that assists individuals in making more informed privacy

Workshop on Usable Security (USEC) 2019
24 February 2019, San Diego, CA, USA
ISBN 1-891562-57-6
https://dx.doi.org/10.14722/usec.2019.23016
www.ndss-symposium.org

decisions about the apps installed on their phone. The idea behind our prototype is to facilitate awareness and transparency among a trusted community of smartphone users to help them make mobile app privacy decisions collaboratively. The following research questions guided this research:

- **RQ1:** *Would smartphone users find features that supported social interactions for making mobile app privacy decisions collaboratively with others useful or not?*
- **RQ2:** *What would motivate them to think about and act on privacy and security issues for themselves and for others?*

To answer these questions, we conducted a design probe study with 10 participants who interacted with our app prototype on smartphones we provided. Through this study, we first aimed to understand how participants made decisions about their app permissions currently and if they sought advice from others regarding these permissions. Then, we had each participant interact with our app prototype and answer questions regarding various features designed to promote social processes for making informed privacy decisions. Overall, we found that participants did want advice from others on how to manage their app permissions; however, they may refrain from advising others if the situation did not directly benefit them. We also found that users appreciated the advice from expert/certified users more than trusted friends or family members. Based on our findings, we make the following unique research contributions:

- A novel app prototype design that promotes social processes to help people make app permission decisions with others;
- An evaluation of whether such an app would be well-received by users; and
- Identification of key factors that affect participants' desire to help others.

While previous studies have confirmed the value of leveraging social processes in privacy decision-making [11], our study is one of the first to conceptualize a tool that incorporates these social features into the design of an app prototype that helps users collaboratively manage their mobile app privacy permissions.

II. BACKGROUND

In this section we first introduce app permissions, risks associated with them, and prior research that has been proposed to help users understand these risks. Then, we discuss our new approach of using collaborative feedback to aid users in making more informed privacy decisions with the help of others.

A. Mobile App Privacy Permissions

Most mobile apps are internet-connected and collect personal data, such as contacts, emails, pictures, location, etc. This can lead to situations where personal data can be compromised. Whenever smartphone users install a new app, they can either allow or deny permission to access key information from the phone (e.g., location, contacts, making phone calls, etc.). Certain permissions are requested at run-time, as opposed to during installation, when the app needs a resource in order to function [12]. On Android, an app's manifest file lists all the resources to which the app requests access to and for which the user has granted or denied permission [13].

While users are notified when an app requests permission to their personal information, Kelley et al. [7] found that these permission notices often leave users confused and unable to fully comprehend the implications for their privacy. People may read this information, but most of the time they do not understand what they have read and are unaware of why the app is requesting access to particular resources [13]. Votipka et al. confirmed that when the reason for resource access was unclear, people tend to assume that their personal information is being accessed and used in contexts that they are more comfortable with than is actually the case [14]. These findings challenge the notion that users are able to give meaningful informed consent when allowing or denying app permissions. Felt et al. [15] found that the majority of Android users did not pay attention to or understand permission warnings and only 20% of their study participants were aware of permissions and scored highly on a comprehension metric. As such, malicious apps may steal personal data, payment details, and other sensitive information.

There have been several studies which focus on improving the security information of apps to help users make informed decisions. For example, Gilbert et al. developed AppInspector, an automated validation system that analyzes apps and generates reports on potential privacy and security violations [15]. Others proposed several extensions, including MockDroid [16], TISSA [17], AppFence [18], and ProtectMyPrivacy [19], which replace private information with false data into the API calls made by apps so that apps can still function without compromising users' personal data. Based on observed user expectations and comfort regarding resource accesses by apps, others have made design recommendations for improving user understanding of privacy in apps and mobile-privacy systems [14], [20]. While these studies enhanced the privacy of individuals, none of these studies went beyond the individual to share knowledge among trusted groups and help them collaboratively make better privacy decisions. Thus, this is the goal of our current work.

B. Collaborative Privacy Management

Collaborative feedback from trusted members of one's social network can aid individuals in making

informed decisions about their privacy and security [21]–[23]. For example, Dourish et al. found that many users delegate security decisions to those they trust [24]. Goecks et al. proposed a privacy management system that helped individuals manage their cookies based on feedback from the community of users who have previously visited the site [25]. In a study to observe how user actions are influenced by their friends, Das et al. [11] presented Facebook users with announcements prompting them to check on extra security features available to them. They found that an announcement that included a message saying a user's Facebook friends used the security feature being advertised influenced the user receiving the message to explore the feature but not to act on it.

Thus, these prior studies show promise that collaborative privacy management can help individuals change their behavior and make better-informed decisions. However, smartphones that require users to make important decisions about privacy do not yet support such social processes, making it more difficult for smartphone users to make informed decisions about their app permissions. Therefore, a novel contribution of our work is that we investigate whether an app prototype that supports social collaboration could impact how users make privacy decisions regarding apps installed on their smartphones. In the next section, we introduce the design rationale for our mobile app prototype.

III. MOBILE APP PROTOTYPE DESIGN

The purpose of our mobile app prototype is to bring people who know and trust each other (e.g., friends, family, co-workers) together to help one another make privacy decisions for mobile apps. Users are intended to be able to join multiple groups to receive feedback from a variety of people. We chose to prototype for Android due to the ease in of Android deployment and the greater number of permission decisions Android users tend to make. The app mockups were developed in Axure, a high-fidelity prototyping tool that allows for interactive exploration [26]. Since this was an initial exploration of the viability of a novel idea, we chose not to invest time in developing a fully functional app. Instead, we had participants interact with the prototype on mobile phones we provided. As shown in the Figures 1-3, our prototype displays the view for the persona of "Taylor Kim" and his/her family.

Our app includes three main features: 1) the Community Feed, 2) the Discover page, and 3) the App Manager. In designing our main features, our intent was to promote social processes related to increased awareness among community members, and communication around privacy decision-making [27]. The Community Feed contains automatic updates on the privacy decisions of community members as a mechanism for community members to gain awareness of the privacy-related behaviors of others whom they trust. We added comments to the Community Feed in order to enable communication between community members. The Discover page was modeled based on the app search and review features in the Google Play Store, but designed to support collaborative privacy decision-making. The App Manager is based on the app permission manager on Android smartphones and was redesigned with social features to support existing privacy controls. Finally, we incorporated certified users as experts to explore whether users might want experts in addition to trusted community members. The following sections illustrate these features in greater detail.

A. Community Feed

Figure 1 shows the Community Feed, which helps community members directly interact with each other over privacy and learn from each other's decisions. It features automatic updates from all community members detailing what apps they are installing or uninstalling and the permissions they have allowed to an app, both at install-time and at run-time. Users can help other members of their community by

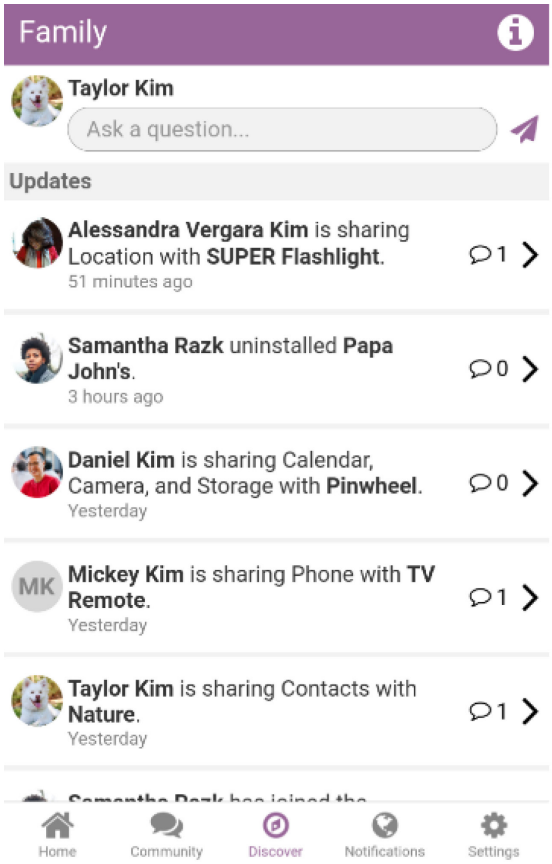

Figure 1: Community Feed

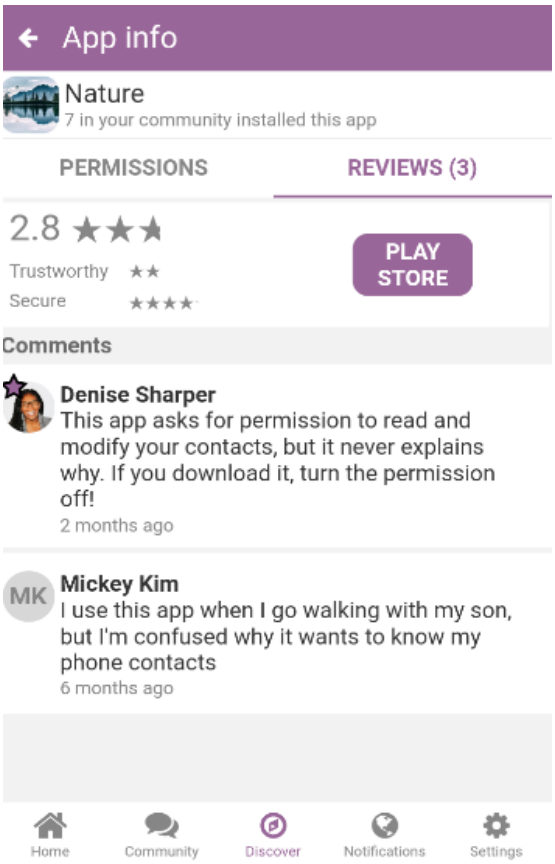

Figure 2: Discover Page

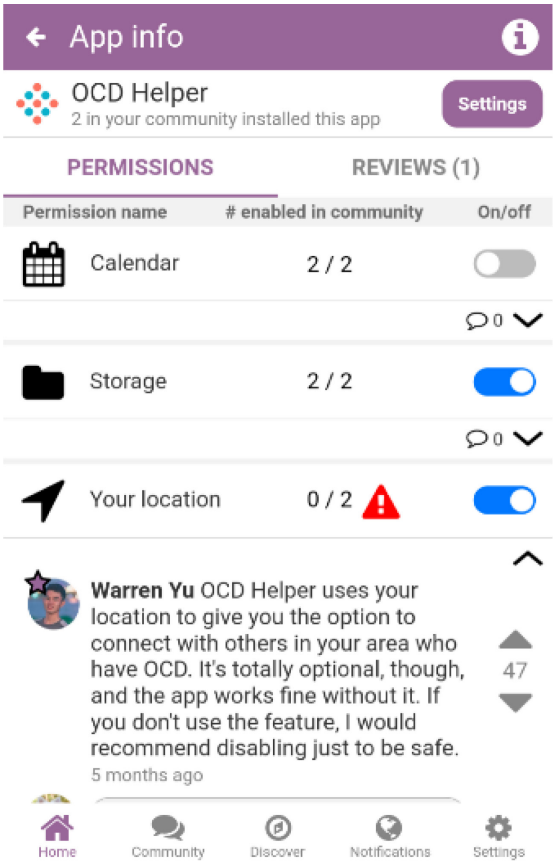

Figure 3: App Manager

commenting on these updates. The comments can then serve as advice or warnings on others' app activities. In addition, users are able to post questions and concerns about apps in order to receive advice from others. Even though the basis of this page is social, as community members are encouraged to talk to one another, it is intended as a forum for privacy-related questions and conversations rather than a social network such as Facebook or Twitter.

Users have the option to be more restrictive and can disable the sharing of particular apps with their community. Disabling sharing for an app means that any decisions the user makes about the app will not be visible on the Community Feed. However, our app itself may still collect this information.

B. Discover Page

On the Discover page, shown in Figure 2, users can leave privacy-focused reviews and ratings on the apps they use, in order to serve as guidelines for other community members. The goal of the Discover section is to eliminate the anonymity behind global review systems generally found in app stores. Without such anonymity, there is no space for paid reviewers or bots to leave reviews designed to boost ratings. Instead, users of this page can feel comfortable knowing reviews were made by people they know and trust. This page also includes a quick link to the app store, which provides users an easy way to purchase or download an app once they have researched whether it is up to their privacy standards.

C. App Manager

As the homepage of the app, the App Manager, shown in Figure 3, displays all apps on the user's smartphone. Users can select a particular app to see an in-detail page with more information, including the permissions it requests, which permissions the user has allowed, and some features to support social navigation. Users can leave comments on specific permissions of specific apps to help other members of their community better understand why apps request certain permissions and manage accordingly. From the App Manager, users are also able to control which apps are shared with the rest of the community and which they would like to keep private or hidden from their community members.

Drawing from previous research on social navigation for privacy, we included a feature that displays how many members of the user's community who own the app have allowed each permission. As Besmer et al. found this kind of community information impacts user decisions only when the visual cue is strong [28], a red warning sign is

displayed when only 50% or less of the relevant community has allowed a permission that the user has allowed. This feature is intended to help people make more educated decisions by leveraging the privacy decisions of others in the community. However, if users have chosen to disable an app from being shared with others, they will not be counted in any of the social cues provided to others.

D. Certified Users

Since we recognized that small communities of friends and family members may lack expertise in digital privacy, we introduced the concept of certified users, presented in Figure 4. This feature gives certain users the designation of being an expert in privacy and security. These users, called certified users, are able to leave reviews on apps and specific permissions that will then be made visible to everyone. Despite this, certified users are unable to see comments from groups for which they are not members.

In the completed version of the application, we plan to implement a setting that allows one user to be the moderator or admin of the community in order to keep discussions relevant to app permissions and security. Moderators will oversee users' comments and prevent misuse of the app, such as cyberbullying or spam. They also have the authority to pin questions to the top of the feed for a certain amount of time if they find them helpful to others. These moderators are intended to be the only ones who are able to add others to the community that they moderate. We are also exploring the idea of users having the ability to block others from viewing their posts and updates, to keep them in control of their privacy.

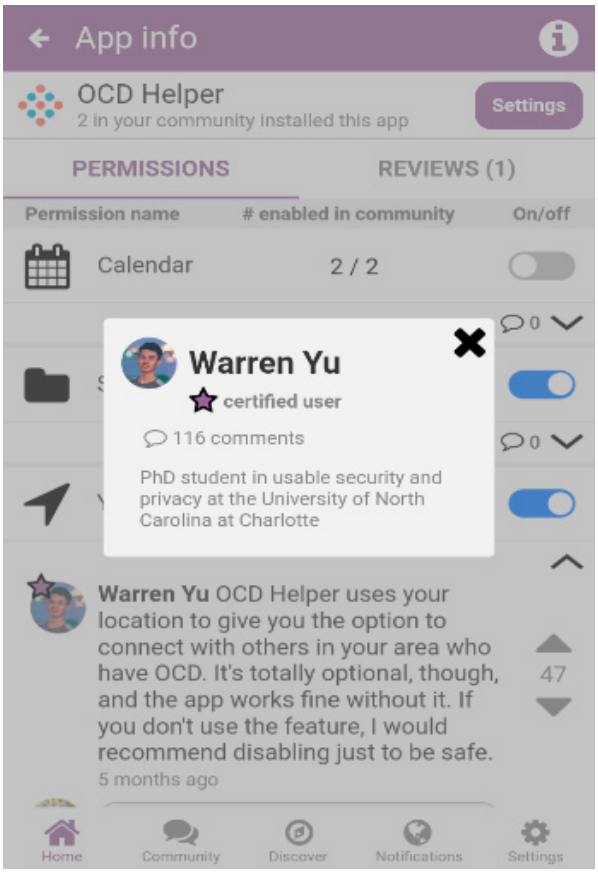

Figure 4: Certified Users

IV. METHODS

This study was a part of a summer Research Experience for Undergraduates (REU). The entire study lasted nine weeks, including prototype design, study design, IRB approval, recruitment, design probe sessions, and analysis.

A. User Study Design

We chose to use a high-fidelity prototype of our app because this study was an initial exploration to assess the viability of a novel design concept for social collaboration in privacy decision-making in the unique context of mobile app permissions. We wanted people to have a good sense of interaction because the idea is so novel. Therefore, we chose to use a high-fidelity, interactive prototype because it gave users a more tangible idea of how a final version of this app would work [29]. A low-fidelity prototype would not have provided as much realism and interactivity; thus, it may have limited participants' feedback about the design features.

We began our user study with background questions about mobile app permissions. We prompted participants to look through the app permissions in their own phone's settings, and we asked how they make decisions to allow or deny permissions. We then asked participants questions to gauge whether they incorporated any social processes in their decision-making about privacy and security settings, such as receiving help from others, giving help to others, or discussing related issues with others. We continued by giving participants an Android phone with our app prototype open and guiding them through three scenarios to follow while interacting with the prototype.

For the scenarios, participants were asked to pretend they were Taylor Kim, a fictional character using our app in a community consisting of 20 extended family members. Participants were able to explore our app as they wanted in order to have a better idea of all the features included and how they functioned. After participants finished interacting with the prototype, we asked questions focused on the usability of the app. From this, we wanted to gain insight relating to the ease of use, which features would help users make better decisions, and which features were unnecessary.

After the three scenarios, we asked users a few follow-up questions about their experience with the app and about any suggestions they had to improve

our design or features. We thanked them for their time and gave them gift cards. Each user study was conducted in a private room with two researchers. Each session lasted about an hour. We recorded audio of each session and transcribed the interviews verbatim for qualitative coding. In the next sections, we describe the scenario-based explorations the participants engaged in during the study.

1) First Scenario: Discover

In our first scenario, we prompted participants to search for an app called *Nature* on the Discover page. We asked them to read reviews of the app from community members and decide if they would download it, based on the reviews. In this scenario, we also introduced certified users to see if participants would be more inclined to listen to their advice over the advice of members of Taylor's community. Once participants finished interacting with the Discover page, we followed up by asking the following questions:

1. Would you look up an app here before downloading it?
2. Do you think an app's trust ratings or reviews would influence your decision to install it?
3. If you were part of this group, when do you think you would leave your own ratings/reviews?
4. Does being in a closed group of people you know affect your decision to check an app's reviews or leave your own? (vs. the app store, where everyone can see)
5. How do you feel about certified users' reviews? Would you be more inclined to trust certified users' reviews over community members' reviews?

Next, participants explored the Community Feed.

2) Second Scenario: Community Feed

In our second scenario, participants were shown a notification that someone had commented on one of Taylor's updates. We had them tap on it to view the update, which notified the community that Taylor had shared their contacts with an app, as well as a family member's warning comment. We asked participants to go back and view the Community Feed so they could understand what type of updates would be posted and who else would be a part of this community. We presented users with the upvote/downvote feature in the comments on updates. This feature is designed to help users validate others' comments. We then asked the following questions:

1. When or how often do you think you would look at this kind of feed?
2. Would you want a regular reminder to check the feed?
3. How often would you want to get notifications? At what point would it be too much?
4. What other kinds of notifications would you want to get from the feed?
5. In what circumstances, if any, would you comment on someone else's update and vice versa?
6. Do you think it is helpful to be able to upvote and downvote comments? Would you rather have liking and disliking, or something else?

Next, we introduced participants to the App Manager.

3) Third Scenario: App Manager

Our last scenario involved the App Manager. We began by showing the participant a list of apps on Taylor's phone. One of the apps included was titled *OCD Helper*, which Taylor did not want to share with the rest of his/her family, because it was personal. We asked participants to disable sharing for this app and then look through the social cues we implemented in *OCD Helper*'s in-detail page. This is where participants could see which permissions others in the community had allowed or denied. Participants also encountered certified users again here when viewing comments on specific permissions. As we wanted to learn how the design could be as clear as possible for users to understand the social cues, we focused some of our questions for this scenario on the interface. We asked the following questions:

1. On the app permissions page, is it clear what the different features are?
2. How could this page be more clear or interactive to you?
3. Would knowing how many other members had enabled a permission influence your decision to enable or disable it?
4. If you have a permission enabled and someone leaves a comment on that permission, would you want to receive a notification?
5. Would you want more explanations for what these permissions are?
6. Do you feel like there is enough information here to make informed decisions about privacy settings?

B. Participant Profiles

Participants were required to be at least 18 years old and to own a smartphone. We recruited a convenience sample of ten participants within a university setting. First, we recruited participants who were participating in other summer REU programs on campus. Then, we also recruited participants at the entrance of the university library. We offered a five-

ID	Age	Sex	Smartphone
P1	22	M	Android
P2	19	F	iPhone (Former Android User)
P3	20	F	Android
P4	35	F	iPhone (Former Android User)
P5	21	F	iPhone (Former Android User)
P6	22	M	iPhone
P7	19	M	iPhone
P8	20	F	iPhone
P9	28	M	Android
P10	21	M	iPhone (Former Android User)

Table 1: Participant Profiles

dollar Starbucks gift card for an hour of participation. We received IRB approval to conduct this study. Table 1 shows participant demographics.

V. RESULTS

Overall, participants were generally positive about our app design. After completing the three scenarios, nine out of our ten participants said they could imagine using the app, although P3 & P10 qualified their answers by stating that they probably would not use it often or consistently. We followed up by asking which parts of the app participants saw themselves using. A full breakdown of their positive responses (i.e., they would use this feature) is shown in Figure 5 and described in more detail in Section A.

Based on our initial questions, most participants seemed familiar with mobile app privacy permissions and made contextual decisions based on the app as to whether they would accept or deny permissions. For instance, P6 specified if it was a well-known app they would usually accept:

"I guess if it came up expectedly, if it's an app that I usually know, then I'll do it. If it's a random app, I'm like, 'What is this?' Then I'll be like, 'Why is this asking for my location if I don't even know like how I got to this app?' So, if it's like, you know, a trusted app that I already know, then I'm like, 'Okay, it's cool.' It's just Google, or it's Apple, or something."

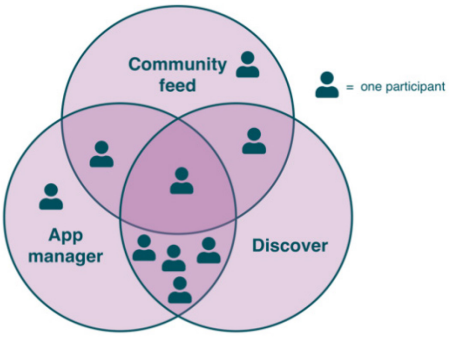

Figure 5: Which features do you see yourself using?

In contrast, P8 would only accept permission requests if it was convenient or necessary for the app:

"It depends on the app, necessarily. If it's like necessary to have a current location, or helpful, I'll do it, and if not—if it's like, you're shipping something one time, or if it's not a regular use of it—I won't give it to them. Mostly, if it's going to be a huge convenience, I'll go ahead and do it. And if it's not gonna add that much time saved, or whatnot, I won't. I'll just type it."

However, one participant (P4) accepted permissions regardless of the request and app because they did not understand what the app was requesting:

"Yeah, we just download and use it. Sometimes maybe there are many requests, sometimes the app needs many information about us, but I don't care. Because if we don't allow it to use all our information we can't use the app free [sic]."

Next, we summarize participants' evaluation of the specific features of the app prototype.

A. App Feature Evaluation (RQ1)

The App Manager and Discover features were the best-received among participants, with 7 participants saying they would use the App Manager and 6 responding affirmatively about the Discover Page. Although we intended the Community Feed to be the core feature of the app, only 4 participants said they would use this feature. One participant said they did not find any of the app features useful.

While participants expressed disinterest in the Community Feed, there was still some positive feedback. Overall, participants expressed increased trust in the app because of the community aspect of our prototype. P5 explained that they would find reviews from within a community more trustworthy:

"*If I actually know these people and trust them and know that they're real and good people*."

P1 mentioned that the Community Feed would help them be more aware of what permissions they are accepting:

"*I very much like how in the [Community Feed], where people have the questions and whatnot, I like this. People say they allow the location, and somebody asks, 'why did you do that?' Or 'please be careful.' If I had enabled it, then I'll be 'oh, wait a minute. I didn't know this.' I'll probably start thinking whether I should have it allowed or not."*

However, most participants expressed an overall disinterest in using the feed. P5 said:

"I don't know if it's really for me because I don't know if I care enough."

Meanwhile, others expressed concerns about "oversharing," "privacy," and "creepiness," which

made them more negative about the Community Feed. For example, P10 said:

"*I don't know if I want people to know what I'm doing. I just don't like sharing stuff."*

In contrast, the Discover Page was more popular among our participants because it did not require automatic sharing of which apps users installed or the permissions they granted. Participants also liked that this feature focused on trusted connections, rather than the public. P6 mentioned specific interest in the Discover Page for this reason:

"*Yeah, I mean, sounds pretty cool. Like, if I could specifically see people I actually know—'cause, I mean, you don't really know when you're reading a regular app, the reviews—a lot of people are like, 'Yeah, this was written by employees,' or something like that. I've sort of seen a few apps where—I saw something yesterday on the app where [trails off]. 'Don't trust any of these five-star reviews. It's written by employees.'"*

Other participants expressed similar sentiments about this feature being more useful because it was beneficial for people they cared about. When we asked P5 if they would be more inclined to leave reviews on this app as compared to public reviews, they responded:

"Definitely, yeah. I don't think I would care for like a stranger. But if I were to tell my siblings or my friends in person if I cared enough to do that. I would do it on this app too."

Similarly, 7 out of 9 said they would use the App Manager feature. Participants thought it would help them make decisions about permission settings they may not have been sure about. P9 said:

"I would definitely see myself using like the summary of who has enabled what permission to what app."

Participants felt that it was valuable to know whether people they knew chose to grant or deny various app permissions. Within the App Manager, a symbol is shown to capture the user's attention if no other members of the community granted a particular permission to a given app. When asked if the number of people having a certain permission enabled would affect their decision to enable or disable a specific app permission, P7 explained:

"It would. Especially with this big zero out of two and the big exclamation point. Like, hey, this is actually something that's different."

Finally, even though participants liked the idea of family members helping one another, many participants also mentioned certified users as a positive feature that allayed concerns about their personal networks lacking the expertise needed to make good mobile app privacy decisions. P1 said:

"*Because she [a certified user] dabbles a little bit more into technology than, let's say, my fifteen family members whose interests may span outside of technology, then I would take her word for it a little bit more*."

Further, participants were concerned that people in their personal networks might not be motivated enough to help one another, and they expressed that certified users could fill this gap. P5 said:

"*Having certified users is a really good tool, I think, because not all your friends and family members might even bother to [leave reviews]. They might look at it, but they might not add a review."*

In the following section, we delve deeper into the notion of community participation and the motivation to work together to make mobile app privacy decisions.

B. Motivation to Help Others (RQ2)

When we asked participants when they would help others or want help making decisions about mobile app permissions, 7 of the 10 participants would only help or want to be helped when it directly affected them. For example, P5 explained that she would only use the Community Feed to gain knowledge about the apps she had:

"If it wasn't an app that I had, I don't think I would care. I would use it for the apps that I have."

However, she did also say that she would comment on someone else's update in the feed:

"If it relates to me, if I'm with them and it shows their location settings, or maybe like if they have my information on their phone or certain things about me."

P7 gave an example of a family member sharing their contacts with an untrusted app and explained that he would comment on someone else's update:

"*When it would directly affect me, and then when it also affects people closer in the community to me. So, like, my mom, my dad."*

However, when we asked P9 when he would comment on updates he saw as concerning, he explained:

"Yeah in that case I mean that's a red flag I think so I'd say like 'Hey, are you sure you want to share your location with your flashlight?'"

Our original idea about a group of users helping one another relies on the assumption these users are willing to help each other when they can. However, as we observed over the course of this study, users were not as motivated to help others unless it directly affects them. This unanticipated factor will be a key challenge to focus on moving forward.

VI. DISCUSSION

The feedback participants gave us indicates that the social features we propose could potentially be useful, and thus will merit deeper exploration. We discuss what lessons we learned about motivating users to help others, their trust in other people's decisions and feedback, and limitations and

modifications to our design. The most useful social mechanisms may be those incorporated into existing platforms and decisions processes, and thus we hope our exploration can also provide insight into the design of community features to support privacy advice and social support more broadly.

A. How Do We Motivate People to Help Others?

Before this study began, we hypothesized that people would be more motivated to help those closest to them, and therefore we based the prototype on a community of family members. However, even with this design choice, our participants expressed less willingness to help family members than we anticipated. Participants expressed reluctance to pay attention to the ongoing decisions and updates from others when there was no personal stake in those decisions, even though they might appreciate such help themselves. Thus, the Community Feed was not as well received by participants as other features. Therefore, an open question remains as to how to motivate users to do the additional work of interacting with others over time, and in what contexts users are more likely to provide such feedback.

Still, users stated that they were much more likely to help those they know and are close to than strangers. Thus, social processes involving such interaction and feedback are more likely to occur in close communities, as opposed to networks of strangers. For example, some participants said they would be more willing to leave comments on the apps they have downloaded in our app, rather than public reviews, because they knew those comments would help and only be visible to people they know. Participants seemed fairly comfortable with the Discover page and the notion of leaving this explicit feedback on their apps and viewing the feedback left by other family members. As such, our research provides initial validation that designing for and leveraging social processes to help people within a community setting work together to make mobile app privacy decisions is worthy of further exploration.

B. Who Do People Trust to Help Them Make Privacy Decisions about Mobile Apps?

Trust emerged as an important factor in our study. Participants compared the Discover page to app stores, where it is difficult to know who is leaving reviews and comments about a particular app. Within a community, participants knew that the feedback was provided by people they know and trust, which they liked. However, this also came with drawbacks, as participants discussed how their friends and family are not very knowledgeable about privacy and mobile apps. So, while they may trust these individuals' motives, they were concerned about the quality of their advice.

Instead, participants explicitly discussed the benefits of having some sort of "expert" participating in the community. We were purposefully vague on how that expertise would be determined and whether or not this expert was known to the user. Many participants interpreted the expert as someone outside of their social network who could fill in the gaps of knowledge of their own community. Trust in this person was still important, as participants clearly wanted an unbiased, yet knowledgeable, opinion they could rely on. However, it was less clear how this trust would be built to ensure that the source was reputable. These results indicate that finding mechanisms for providing trusted privacy guidance that users feel confident in would be valued. We need to further examine how to determine such experts, their incentives for participating in such a system, and how other users would want to interact with them.

C. Implications for Redesign

There were several concerns with the design of our prototype that participants raised. They wondered how useful some of the information would be to them, given that they might use apps that other members of their community do not. We hoped the Community Feed would provide awareness of app usage beyond a user's own apps, but participants were not really interested in sharing such information. Some participants also expressed reservations about oversharing their app behavior, particularly in the Community Feed. Thus, our design needs to make it easy to not share this information, or only share this information with a select few people. Further, we need to examine the structure of this community, and how to balance the trust people would place in those closest to them with the greater breadth of knowledge people would gain from a larger community. Using outside experts may also help alleviate this problem; as such, our design needs to make clear the different interactions one may have with experts versus members of the community.

A repeated concern expressed by participants involved in the App Manager feature. Unlike the Community Feed, which was compared to social media status updates, and the Discover Page, which participants compared to the app store, the App Manager was more novel to participants. As a result, participants had more trouble understanding it than other parts of the app. In general, they liked the idea behind the App Manager, but some were not keen on the design of it. For instance, some participants said it was too cluttered. Others did not understand the purpose of certain features until we explained them. Therefore, we need to find ways of making the App Manager more streamlined and intuitive to understand, perhaps by presenting features in a way that users are more likely to be familiar with. Instead of having all the features on one page for the App

Manager, we have thought to break it up into further subsections. The goal is to have users feel like they are using the settings on their phone. For instance, instead of users viewing all the information we provide on one page they can click on each permission which takes them to the extra social features our app would provide. This would address the concern of clutter on the screen and also help users connect it to something they're already familiar with.

Finally, participants expressed the desire for more information to be given about what permissions entailed in the App Manager. Our design would benefit from giving users the ability to easily view what personal data was encompassed by a permission and how it is commonly used.

VII. LIMITATIONS

The main goal of this study was to get initial feedback on the novel idea of leveraging social collaboration as a means for making privacy decisions in the context of mobile app permissions. However, the time constraints of the summer REU were a major limitation of this study. Because we only had nine weeks for the entire study, this constrained the number and types of participants we recruited, as well as some of our study design choices. Still, we believe this early feedback is valuable for the HCI and usable privacy and security communities, as we move forward to examine deeper questions by developing and deploying such social mechanisms.

Also, since we recruited a convenience sample of students who may have been inclined to provide positive feedback about our app features, we focused our analyses on whether and how aspects of awareness, transparency, trust, and privacy decision-making embedded within the design of the app influenced how participants viewed these features. By doing this, we were able to uncover interesting nuances regarding whom users trust and their general lack of motivation for helping others. Yet, we acknowledge that demand characteristics [30] may still have influenced participants to respond in a way that they thought aligned with our expectations. In future studies, we will consider methods of obscuring the researchers' role in designing the app, in order to mitigate bias. We will also expand our population beyond students and investigate a broader range of participants and communities.

VIII. CONCLUSION AND FUTURE WORK

We explored how users feel about integrating their community with privacy decision-making processes in order to help one another. After designing an app prototype that we felt would help users, we conducted a study to observe reactions and gain insight from different perspectives. Although we anticipated participants would want more interaction between users, we found that participants were more likely to keep information to themselves, unless they were directly affected by others' actions. It is important to note that, overall, participants said that they found our tool useful and would use it in real-life settings. However, there is still much work to be done to study how people could be motivated to take part in such a community for sustained use.

To build upon this initial exploration, we are currently conducting a participatory design study with more diverse groups of two or three people who know one another (e.g., family members, friends, co-works), so they can help us design new features that support social collaboration for privacy decision-making for app permissions. We aim to continue to examine how social processes can support privacy and security decision-making, so people can help and support each other.

ACKNOWLEDGEMENTS

This research was supported by the U.S. National Science Foundation under grants DUE-1461166 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] "Why does it still take six months for a company to spot a hack?" *NBC News*. [Online]. Available: https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881. [Accessed: 22-Nov-2018].

[2] "Big Idea: Technology Grows Exponentially," *Big Think*, 21-Mar-2011. [Online]. Available: https://bigthink.com/think-tank/big-idea-technology-grows-exponentially. [Accessed: 26-Nov-2018].

[3] K. Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *The New York Times*, 19-Mar-2018.

[4] "Smartphone Security | Mobile Devices are the Most Vulnerable," *Zimperium Mobile Security Blog*, 22-Jun-2018.

[5] "Record shares of Americans have smartphones, home broadband," *Pew Research Center*.

[6] R. E. Crossler and F. Bélanger, "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors," Jan. 2017.

[7] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone," in

Proceedings of the 16th International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2012, pp. 68–79.

[8] J. Aarstad, M. Selart, and S. Troye, "Advice Seeking Network Structures and the Learning Organization," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2420898, Apr. 2014.

[9] R. Cross, S. P. Borgatti, and A. Parker, "Beyond answers: dimensions of the advice network," *Soc. Netw.*, vol. 23, no. 3, pp. 215–235, Jul. 2001.

[10] D. Krackhardt and J. R. Hanson, "Informal Networks: The Company Behind the Chart," *Harvard Business Review*, 01-Jul-1993. [Online]. Available: https://hbr.org/1993/07/informal-networks-the-company-behind-the-chart. [Accessed: 24-Jul-2018].

[11] S. Das, A. D. I. Kramer, L. A. Dabbish, and J. I. Hong, "Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation," 2014, pp. 739–749.

[12] "Permissions overview," *Android Developers*. [Online]. Available: https://developer.android.com/guide/topics/permissions/overview. [Accessed: 08-Jan-2019].

[13] windows-sdk-content, "Application Manifests." [Online]. Available: https://docs.microsoft.com/en-us/windows/desktop/sbscs/application-manifests. [Accessed: 26-Nov-2018].

[14] D. Votipka, S. M. Rabin, K. Micinski, T. Gilray, M. L. Mazurek, and J. S. Foster, "User Comfort with Android Background Resource Accesses in Different Contexts," presented at the Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018), 2018, pp. 235–250.

[15] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A Survey of Mobile Malware in

d Security, New York, NY, USA, 2012, pp. 6:1–6:17.

[22] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," *J. Cybersecurity*, vol. 1, no. 1, pp. 121–144, Sep. 2015.

[23] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 272–288.

[24] P. Dourish, E. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the Wild: User

the Wild," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, New York, NY, USA, 2011, pp. 3–14.

[16] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "MockDroid: Trading Privacy for Application Functionality on Smartphones," in *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, New York, NY, USA, 2011, pp. 49–54.

[17] J. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, M. A. Sasse, and Y. Beres, *Trust and Trustworthy Computing: 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011, Proceedings*. Springer Science & Business Media, 2011.

[18] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These Aren'T the Droids You'Re Looking for: Retrofitting Android to Protect Data from Imperious Applications," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2011, pp. 639–652.

[19] Y. Agarwal and M. Hall, "ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing," in *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, New York, NY, USA, 2013, pp. 97–110.

[20] K. Micinski, D. Votipka, R. Stevens, N. Kofinas, M. L. Mazurek, and J. S. Foster, "User Interactions and Permission Use on Android," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2017, pp. 362–373.

[21] E. Rader, R. Wash, and B. Brooks, "Stories As Informal Lessons About Security," in *Proceedings of the Eighth Symposium on Usable Privacy an*

Strategies for Managing Security As an Everyday, Practical Problem," *Pers. Ubiquitous Comput*, vol. 8, no. 6, pp. 391–401, Nov. 2004.

[25] J. Goecks and E. D. Mynatt, "Supporting Privacy Management via Community Experience and Expertise" To appear," in *in Proceedings of 2005 Conference on Communities and Technology*, 2005, pp. 397–418.

[26] "Prototypes, Specifications, and Diagrams in One Tool | Axure Software." [Online].

Available: https://www.axure.com/. [Accessed: 19-Nov-2018].

[27] H. R. Lipford and M. E. Zurko, “Someone to Watch over Me,” in *Proceedings of the 2012 New Security Paradigms Workshop*, New York, NY, USA, 2012, pp. 67–76.

[28] A. Besmer, J. Watson, and H. R. Lipford, “The impact of social navigation on privacy policy configuration,” in *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS ’10*, 2010.

[29] “Prototyping 101: The Difference between Low-Fidelity and High-Fidelity Prototypes and When to Use Each,” *Adobe Blog*, 29-Nov-2017.

[30] N. Dell, V. Vaidyanathan, I. Medhi, E. Cutrell, and W. Thies, “‘Yours is better!’: participant response bias in HCI,” in *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI ’12*, Austin, Texas, USA, 2012, p. 1321.