Interdependent Privacy in Smartphone App Permissions

JENS PHANICH*, University of Utah, USA
MANILA DEVARAJA*, University of Utah, USA
SHARATH SATISH*, University of Utah, USA

In today's interconnected world, the data stored on personal devices is often not only about the individual but also shared with others through photos, contacts, documents, and more. When applications request access to specific data, users unintentionally expose information related to others on their devices, raising privacy concerns, as the affected individuals are typically unaware and unable to control their exposure. This research study replicates a previous study on interdependent privacy [16] to investigate individuals' privacy concerns, both for themselves, for others, and for themselves from the perspective of others in relation to smartphone app permissions. Using an online survey targeted at undergraduate university students, we found that participants were more concerned about protecting their own privacy than that of others. Furthermore, privacy concerns varied based on the type of permission requested. We found that results also indicated that individuals were more responsive and sensitive to the privacy of others when they were informed that the requested data included information related to others. These findings contribute to the growing field of interdependent privacy and suggest potential design improvements for app permission interfaces to better address users' privacy concerns.

CCS Concepts: • **Security and privacy → Usability in security and privacy**.

Additional Key Words and Phrases: Smartphone permissions, User Experience & Usability, Privacy & Security

ACM Reference Format:

Jens Phanich, Manila Devaraja, and Sharath Satish. 2018. Interdependent Privacy in Smartphone App Permissions. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 28 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

We store an increasing amount of private information of others we interact with on our smartphones. As a consequence, the privacy decisions we make no more just impact us but it also impact others and might expose their private information. The official term used to describe the interconnected nature of privacy, where an individual's privacy is influenced not only by their own actions and data but also by the privacy decisions and data shared by others, is interdependent privacy [12].

In the context of smartphones, interdependency matters with regard to the other's data stored on devices and the choices made through smartphone permissions to share this data. Given the vast amount of information shared through smartphones daily, most individuals have little control over how others share data via app-specific permissions.

*These authors contributed equally to this work.

Authors' Contact Information: Jens Phanich, u0916721@utah.edu, University of Utah, Salt Lake City, Utah, USA; Manila Devaraja, Manila.Devaraja@utah.edu, University of Utah, Salt Lake City, Utah, USA; Sharath Satish, u1471908@utah.edu, University of Utah, Salt Lake City, Utah, USA.

Manuscript submitted to ACM

Additionally, they may not be aware of how much of their information—such as photos, shared calendar events, and contacts—gets stored on other people's devices and could potentially be shared through these permissions. The previous research captured the interdependency nature of smartphone permissions through a scenario-based study [16]. The study showed that people are more mindful of others' privacy-sensitive information on their smartphones when they are informed about it beforehand. However, this consideration varies depending on the specific permissions involved.

The recent developments have taken a detour from smartphones to other technologies like smart technologies like smart rooms and drones [1, 21] and LLMs [4, 24]. However, the shift in the focus fails to see the importance of growing concern in data sharing practices on smartphones. Given a lack of user awareness on this issue and the absence of risk signaling [12], it is essential people are educated on the topic of interdependent privacy in a principled manner [16].

This study aims to replicate the findings from [16], focusing on university students to gauge their awareness of others' privacy-sensitive information when dealing with smartphone permissions that risk revealing or sharing that information. In this study, we examine how privacy awareness changes when understanding the potential negative effects smartphone permissions could have on others' private data on their smartphones. In addition to the work by Marsch et al. [16], which had three permissions (Contacts, Calendars, Photos), we are adding another permission, File system, which could also potentially consist of other individual's private files.

To understand the mechanisms and factors influencing a user's privacy decisions that could affect the privacy of others' information when granting app permissions, we borrow the three research questions from Marsch et al. [16] and add another research question (RQ4):

- **RQ1:** Do individuals consider the privacy of other people when making decisions pertaining to smartphone app permissions?
- **RQ2:** Does presenting information cues that feature other people prime users to give greater consideration to the privacy of others when making decisions pertaining to smartphone app permissions?
- **RQ3:** Do concerns for the privacy of other people vary based on the type of permission (specifically, calendar, contacts, photos, and file system) requested by a smartphone app?
- **RQ4:** Do individuals think it is important for others to consider their privacy when giving permissions to smartphone applications?

By answering these, Marsch et al. [16] show that people tend to care less for other's privacy than their own privacy. Hence, we added RQ4 to explore whether individuals expect others to protect their privacy. Incorporating this research question allows us to compare users' perceptions of their own privacy, their views on others' privacy, and their expectations of how others should safeguard their privacy.

We conducted a survey with n=32 students from an undergraduate Ethics of Data Science course at the University of Utah. We found our results similar to Marsch et al. [16], with an individual caring about their privacy more than others. For RQ4, we found that there was not a significant expectation from individuals from others to protect their privacy. Even with an addition to the permissions, for RQ3, we did not see a significant difference in concerns between permissions. This could all be attributed to the low number of participants in comparison with the original study, which had n=633. We believe it is not justified to compare the results of our study with the original due to the limited participation in our research.

2 Related Works

This related works section discusses interdependent privacy and class material and how they relate to our replication study. Since the original paper considerable progress has been made in defining user types regarding interdependent privacy. New technology domains such as smart environments and LLM are being looked at through an interdependent privacy lens and finally, a wide breadth of design solutions have been created to prevent interdependent privacy breakdowns. This related work serves to show strong support for our research questions.

2.1 Understanding Users in Interdependent Privacy

The majority of the work is done to understand users and interdependent privacy through the context of social media. Hasan et al study which looked at social media defined three core characteristics in users regarding interdependent privacy, privacy preservers, ignorers, and violators [3]. Privacy preservation is a characteristic in which users are conscious of potential interdependent privacy violations, ignorers are those who are oblivious to the interdependent privacy concerns. Violators are those who knowingly undermine the privacy needs of others through the data that they share. The underlying motivation behind violators is widely varied, one work in the context of photo sharing found that those with self-deprecating humor were more likely to share sensitive photos of others if they found it funny [10].

Those on the receiving end of privacy violations take it upon themselves to mediate these violations. Users' actions are on the user level and include blocking, unfriending, and self-censorship [17]. It has also been found that users have little confidence in reports, automatic detection, or even legal action and view them as less effective than user-level actions [17]. This finding and the findings in the paragraph above give further motivation for **RQ4**, particularly to see if smartphone privacy permissions are subject to the same user behaviors as social media.

2.2 New Technological Domains of Interdependent Privacy

Exploring the interdependent privacy needs surrounding smartphone use is important, smartphones have been embedded and ingrained into our daily functions for more than a decade. New technologies such as smart rooms, and Large Language Models (LLMs) have seen increased and unprecedented adoption, as such interdependent privacy research looking at these new domains has also proliferated to the point where many of their findings are useful to apply in the context of smartphones. This section shows the gaps in interdependent privacy research regarding smartphones by looking at other domains.

2.2.1 LLMs and Interdependent Privacy. LLMs have seen increased adoption. Questions surrounding the data they contain and how they are trained is a hot topic. Research has found that LLMs contain interdependent privacy concerns [4][24]. Training data is often collected from users in a nontransparent manner, often in ways that give rise to interdependent privacy violations, additionally, the way user data is cleaned of sensitive information is not sufficient [4]. As the demand for data to train LLMs increases so do the methods in which data is collected. One data collection vector that shows promise in training LLMs is smartphone app data [26]. Thus interdependent privacy violations occurring from smartphone app permissions have the potential to work their way into public LLMs. The rise of LLMs and their interdependent privacy concerns workshows the importance of understanding user behavior surrounding interdependent privacy in smartphone app permissions.

2.2.2 Smart Technologies and Interdependent Privacy. Recent work regarding Interdependent Privacy and smart technologies, such as smart rooms and drones, has given rise to the concept of the "bystander". A bystander is typically

a person who has little to no relationship with the owner of the smart device [1][21][22]. Recent work has shown that bystanders want a say in how their data is collected and distributed and may go to great lengths to obfuscate the collection of personal data even if they are on other people's property [1]. However, work has shown that bystanders are only focused on a narrow subset of their personal data, particularly audio and visual data, and are unaware of other types of personal data that can be collected by these devices such as health data [21]. Thus with bystanders having motivation to control their personal data, we seek to understand how those with stronger social ties such as a friendship address interdependent privacy concerns.

2.3 Addressing Interdependent Privacy Leakage and Breakdowns

Recent work addresses interdependent privacy breakdowns from two general angles. The first is addressing the person whose privacy was violated needs, and allowing them ways to gain control of their privacy. The second is preventing others from sharing or disclosing personal information on others and designing systems that involve all parties. This section of the related works introduces this aspect of the related work as a useful backdrop for our study, which targets both the individual who is violating interdependent privacy and with the addition of **RQ4**, the person whose privacy is being violated.

2.3.1 Addressing the needs of the violated. Recent work addressing those whose privacy has been violated as a result of interdependent privacy breakdowns has focused heavily on personal sexually explicit pictures shared between parties, either done as a consensual or nonconsensual act. Coduto et all, found that sexting photos between consenting adults in a relationship, and the interdependent privacy concerns surrounding them requires systems with thoughtful defaults such as shared photos being deleted after the breakup, but that current smartphone applications are not designed with breakups in mind, and often keep this sensitive data post-breakup to the dismay of users [7]. Additional work has been done to look at preventing the sharing of sexually explicit images of individuals without their consent[8][9]. One study found that victims found it difficult to be notified by platforms sharing images without their consent and that resolving the issue through the various platforms exposes them to secondary victimization [9]. Another study found that blind users wish to obfuscate certain content they may be in their pictures before they share them, such as sexual products, but that off-the-shelf obfuscation products do not exist for them to easily do so[25]. Though our study does not focus on sexually explicit material, smartphones, receive and distribute sexual material, and as such understanding user views on app permissions is vital in ensuring this privacy across parties.

2.3.2 Preventing Interdependent Privacy Breakdowns. Work has been creating various systems whose aim is to prevent interdependent privacy breakdowns that arise from social media sharing. One common solution is the creation of systems that incorporate the sharing party as well as the party whose information is being shared to prevent multipart privacy conflicts or MPCs. Niksirat et all. employed a Wizard-of-Oz chatbot that proved effective in preventing MPCs, the chatbot collected consent from all parties involved and negotiated and resolved sharing conflicts such as what and how much information was shared [20]. Niksirat et all. in a different paper working with young users of social media, found that involving all parties in a potential MPC was an efficient way in resolving interdependent privacy conflicts [19].

Additional work has looked at giving users the ability to prevent interdependent privacy breakdowns by giving them root-level control of any content involving their data. Allowing others to only see their data if they had permission. One paper employed facial recognition in photos on Facebook and allowed users to set who could see their face in photos even if they were not the one sharing it [13]. Another paper abstracts this idea to a higher level and proposes

a privacy setting on social networks that allows users to own their private data and allows users to control privacy requirements and information flow of this data [23]. In both these works, the ownership of personal data is designed and enforced at the system level as opposed to the real world where ownership of interdependent data is executed between system-agnostic parties.

3 Methods

3.1 Scenario Research Design

The study we replicate Marsch et al. [16] considers smartphone permission surrounding Photos, Calendars, and Contacts against two categories - Non-person (nonpersonal information) and persons (personal information) forming a 3x2 study vignette. Survey participants are presented with one of the vignettes and are asked a series of questions focused on interdependent privacy and the vignette. We keep these categories and vignettes while adding an additional category surrounding file systems and permissions, resulting in a 4x2 study with four permission settings against the two categories. Furthermore, the study Marsch et al. [16] was conducted with participants from Germany. However, in our study, the participants were sampled from the students of the class CS 3390 - Ethics in Data Science conducted by Professor Sameer Patil at the University of Utah.

To further build upon the breadth of the original study, we created one additional scenario with two vignettes accompanying it to the survey. This scenario revolves around the file systems found on phones. The scenario is of a file system containing either person or nonperson data. Proceeding from this scenario, we ask the same follow-up questions seen in the other scenarios but in the context of a mobile device file system.

	Non-persons	**Persons**
Calendar	Classes	Personal Events
Contacts	Companies	People
Photos	Landscapes and Cities	Parties, trips etc,
File System	Lecture notes	Tax returns, Passport, etc.

Table 1. Information presented in the visual depictions in each study condition.

As we introduced a new research question with RQ4. Do individuals think it is important for others to consider their privacy when giving permissions to smartphone applications? We decided to add one additional question to the survey. This question asks if Thomas was the participant's friend would the participant be comfortable with Thomas downloading the app? Like the other questions in the survey we ask, the wording of this question changes depending on the type of application the participant saw in their vignette. We deployed a Qualtrics survey that was given to students. Students received extra credit if they completed the survey and passed the attention check. We had 32 out of 34 participants pass the attention check and fill out the survey. Below is the flow of our survey.

3.2 Survey Flow

Each participant is assigned a random scenario description, as shown in figure 1. Following this they are asked questions surrounding interdependent privacy. After these questions, they were asked questions about their smartphone usage and demographics followed by a feedback and exit survey with a commitment check. Our survey was roughly 50 questions in length and took 15 to 30 minutes for participants to complete

Refer to the appendix for the full survey configuration and questions we ask.

3.3 Survey Sample

Our survey was distributed to 34 undergraduate university students, in contrast to the 665 participants sourced from Amazon Mechanical Turk in [16], where two responses had to be discarded for failing attention checks. In our study, all participants completed the survey within a reasonable time frame, and none of their responses were discarded. Participants were randomly and equally assigned to one of the 8 scenarios designed for the study, with some initial questions specifically targeting the scenario they were assigned to. The distribution across the 8 scenarios was as follows: Calendar Non-Persons = 4, Calendar Persons = 5, Contacts Non-Persons = 4, Contacts Persons = 3, Photos Non-Persons = 5, Photos Persons = 5, File Systems Non-Persons = 4, File Systems Persons = 3.

Of the 32 participants, 23 were male, 7 were female, one identified as non-binary, and one participant chose not to disclose their gender. Regarding ethnicity, 17 identified as Asian, 8 as White/Caucasian, 2 as Asian and White/Caucasian, 2 preferred not to specify, and one participant each identified as Hispanic, Hispanic and White/Caucasian, and Asian, Hispanic or White/Caucasian. All participants were under the age of 26, and the majority either did not wish to disclose their earnings or reported earning less than $20,000 annually. Every participant, except for one, was single or unmarried at the time of answering the survey. A significant portion of our participants were majoring in computer science (N = 16) or data science (N = 6). Interestingly, while participants in [16] had a 2:1 skew towards using Android OS over iOS, the opposite was true for our participant pool. Of the 32 participants, 25 used iOS, while 6 used Android, resulting in a ratio of approximately 1:4 in favor of iOS users.

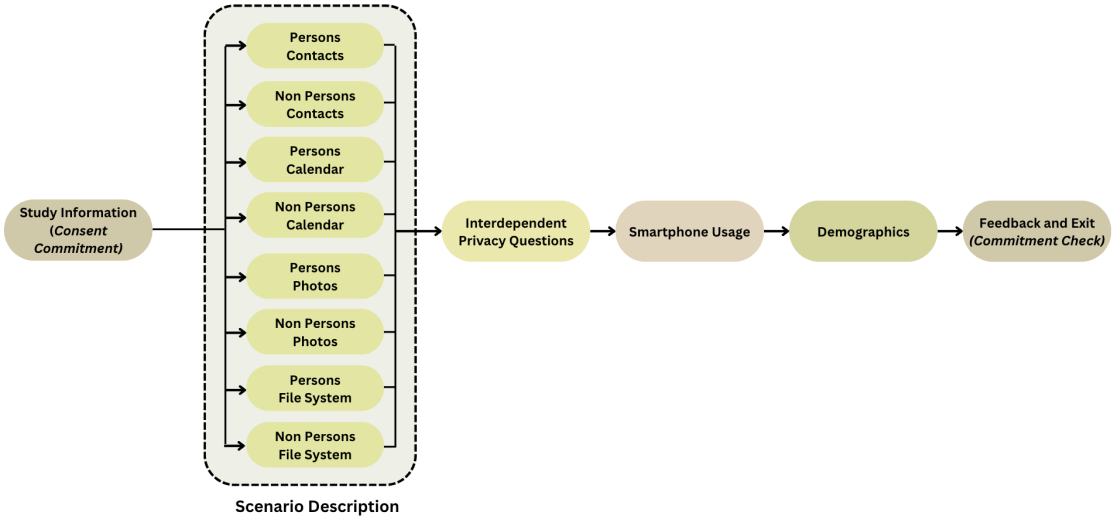


Fig. 1. Survey Flow

4 Results

We analyzed the responses of 34 participants to address the four research questions outlined at the beginning of our study, aiming to understand participants' perspectives on interdependent privacy between Thomas and his friends. However, two participants did not pass the attention checks, and their responses were excluded from the analysis. Building on previous research [16], we calculated the mean and median of responses related to understanding participants' concern for Thomas' privacy, concern for the privacy of Thomas' friends, willingness to install an application that compromises the privacy of either Thomas or his friends, and willingness to install the application from the perspective of Thomas' friends, given that it compromises Thomas' privacy. These analyses were conducted within a scenario-based study focused on the four types of permissions in order to answer the four research questions.

4.1 Privacy Concerns of Friends of Thomas (RQ1)

To understand participants' views on the privacy concerns of others—specifically, the privacy of Thomas' friends—while making decisions about smartphone permissions, we asked participants about their concerns regarding the privacy of Thomas' friends in relation to both the persons and non-persons categories across all four types of permissions. Using ANOVA, we found no statistically significant differences in either the non-persons condition ($F = 3.6486, p < 0.1$) or the person condition ($F = 0.0239, p < 0.8781$). This result contrasts with the original study's findings [16], where ANOVA identified statistically significant differences in the concern for Thomas' friends between the non-persons and persons conditions. While participants reported higher concerns for Thomas' privacy (mean = 4.0325) compared to his friends' privacy (mean = 3.925) in the non-person condition, their concerns were largely similar for both Thomas and his friends in the person condition, with mean values of 3.6825 and 3.7, respectively. This pattern deviates from the findings of [16], where a relatively pronounced difference in privacy concerns was observed between Thomas and his friends in the person's condition. However, a similar pattern emerged in our data, with a larger difference in privacy concerns between Thomas and his friends in the non-person condition compared to the person condition.

We found that the privacy concerns for Thomas' friends were normally distributed for the calendar and photo permissions. Specifically, for the calendar permission, the Shapiro-Wilk tests yielded the following results: Persons condition: $W = 0.82827, p = 0.135$; Non-Persons condition: $W = 0.8173, p = 0.1113$. For photos, the tests showed: Persons condition: $W = 0.83274, p = 0.1458$; Non-Persons condition: $W = 0.89495, p = 0.4064$. However, this normality was not observed for the contacts and file systems permissions in either condition.

For the non-persons condition, the mean values of the privacy concerns of friends of Thomas for permission type were ranked as follows: calendar (mean = 2.75), photos (mean = 3.00), contacts (mean = 3.67) and file systems (mean = 3.75), while their orders changed for the persons condition as follows: calendar (mean = 3.00), file systems (mean = 3.67), photos (mean = 3.80) and contacts (mean = 4.33), as shown in figures 2, and 3. None of the differences were however statistically significantly different. Consistent with the findings of [16], privacy concerns for the calendar permission were lower in both conditions compared to other permissions. Notably, this trend held despite our participants being drawn from a university student population. While similar trends were observed in the non-persons condition regarding concerns for Thomas' privacy, the contacts permission ranked lowest among the permission types in the persons condition.

Fig. 2. Concern for privacy of Thomas for the Non-persons and Persons study conditions for the app permissions: Calendar, Contacts, Photos and Files shown using a violin plot, with higher values indicating higher privacy concern.

Fig. 3. Concern for privacy of friends of Thomas for the Non-persons and Persons study conditions for the app permissions: Calendar, Contacts, Photos and Files shown using a violin plot, with higher values indicating higher privacy concern.

When considering participants' views on whether it was Thomas or third parties' responsibility to protect the privacy of Thomas' friends, we found that, in the persons condition, participants believed it was more Thomas' responsibility (mean = 3.62, median = 4.0) compared to third parties (mean = 3.19, median = 3.5), a similar trend observed in [16]. However, in the non-persons condition, the reverse was true, with third parties being seen as more responsible (mean

= 3.88, median = 4.0) than Thomas (mean = 3.44, median = 3.5), which was not the case in [16]. ANOVA revealed no statistically significant differences in participants' views on this topic.

4.2 Priming Participants on Interdependent Privacy (RQ2)

When participants were introduced to the concept of interdependent privacy through the survey questions, the means for the concern regarding Thomas' privacy across both the Non-persons and Persons conditions, as well as the concern for the privacy of Thomas' friends across both conditions for all four permissions, are presented in Tables 2 and 3, respectively. In contrast to the findings of [16], where priming participants on interdependent privacy increased concerns for Thomas' friends in three of the four conditions (excluding the photos permission), our study did not show the same pattern.

Table 2. Means for Privacy Concern for Thomas for Persons and Non-Persons conditions, with higher values indicating higher privacy concern.

Permission	Non-persons	Persons	Difference
Calendar	3.25	3.80	0.55
Contacts	4.33	3.00	1.33
Photos	4.75	4.33	0.42
File System	3.80	3.60	0.20

However, based on Mann-Whitney tests with Bonferroni corrections, no statistically significant differences were found between the Non-persons and Persons conditions ($p = 0.25$).

Table 3. Means for Privacy Concern of Thomas's Friends for Persons and Non-Persons conditions, with higher values indicating higher privacy concern.

Permission	Non-persons	Persons	Difference
Calendar	2.75	3.00	0.25
Contacts	3.67	4.33	0.66
Photos	3.75	3.67	0.08
File System	3.00	3.80	0.80

When ANOVA was conducted to examine the differences in the intent to install the application requesting a specific permission from Thomas between the Non-persons and Persons conditions, a statistically significant difference was found ($F = 4.909$, $p < 0.05$). However, no statistically significant differences were observed between the permission types within either of the conditions.

In the Non-persons condition, the following intent scores were obtained for each permission type: Contacts (median = 3, mean = 2.67), Photos (median = 3, mean = 2.8), and File Systems (median = 1.0, mean = 1.25). Here lower values indicate stronger reasoning to refrain from installing the app and thereby restricting permission to access information, thus protecting the privacy of Thomas and his friends. In the Persons condition, the following intent scores were obtained for each permission type: Contacts (median = 1, mean = 1.33), Calendar (median = 2, mean = 1.8), Photos (median = 2, mean = 1.8), and File Systems (median = 3.0, mean = 2.67). In all the app permissions, barring permission to

access file systems, participants were less willing to install applications which could jeopardize the privacy of Thomas or his friends in the Persons condition rather than the non-Persons condition. These results are consistent with the findings of [16], where the intent of participants to install apps decreased across all three permission types (excluding file systems, which was not studied) in the Persons condition.

While a similar pattern emerged in our study, with the calendar permission showing the least privacy concerns compared to the other permissions, the result is still interesting given that all our participants were university students. This demographic might be expected to have higher concerns about calendar privacy, but this was not observed in our study.

In addition to examining participants' views on installing applications that request specific permissions, we also asked participants to indicate the amount, in dollars, they would be willing to pay—either on a monthly basis or as a one-time lifetime subscription—to prevent data access from third parties by not granting the requested permission, as shown in table 4, and thus protect the privacy of the parties involved. While the findings of [16] suggested that participants were more willing to pay the application in Persons than in the non-Persons condition, our study shows that the results are mixed, with participants willing to pay more to restrict app permissions Calendar, and File systems in the Persons category, while they were willing to pay more for restricting Photos, and Contacts permission in the other category. In addition, the median values of the amounts that participants were willing to pay across all app permissions and conditions were significantly lower compared to the findings presented by [16]. This difference may be due to the fact that our survey population consisted of undergraduate university students, a group whose values regarding privacy and willingness to pay for privacy protection may differ from those of older age groups.

Table 4. Median and mean amounts in US Dollars that participants were willing to pay to prevent data access.

Permission	**Median**		**Mean**	
	Non-persons	**Persons**	**Non-persons**	**Persons**
Calendar	$0.00	$0.00	$0.50	$3.00
Contacts	$8.00	$2.00	$12.67	$1.67
Photos	$3.00	$0.00	$6.00	$1.25
File Systems	$1.50	$3.00	$2.00	$3.67

4.3 Privacy Concerns by Permission Type (RQ3)

While statistically significant differences were found in the findings presented by [16] on the concern for Thomas' privacy across the app permissions in the non-Persons condition, that was not the case in our study. However, significant differences were found between the permission types regarding participants' comfort with granting access in the Persons category ($F = 4.181$, p-value < 0.01). In contrast, no significant differences were observed between the permission types in the Non-persons category.

From the responses provided by participants who were randomly assigned to one of the eight scenarios in the study, the mean values of privacy concern for Thomas in both the Non-persons and Persons conditions are highlighted in Table 2. In the Persons condition, the privacy concern for app permissions related to Photos, Calendar, and File Systems were significantly different from that of Contacts. However, in the Non-persons condition, the results varied, with Photos, Contacts, and File Systems showing significant differences compared to Calendar.

In addition to exploring participants' views on Thomas' privacy across different app permission types, we also investigated their privacy sensitivity and comfort levels when granting these permissions to applications in both the persons and non-persons conditions. With regards to privacy sensitivity, the mean values for app permissions file systems, contacts and photos was higher than the privacy sensitivity of the calendar permission in both the conditions. The same trend was observed with regards to the access comfort of granting specific app permissions to applications, where participants were least comfortable to share permissions consisting of file systems, photos and contacts in contrast to calendar permission. Similar results were obtained from the findings of [16] in the non-persons condition, where participants prioritized photos and contacts over calendar when it came to privacy sensitivity and access comfort.

Table 5. Privacy sensitivity and Access Comfort by permission type in Persons condition.

Permission	**Privacy Sensitivity**		**Access Comfort**	
	Median	**Mean**	**Median**	**Mean**
Calendar	4.00	3.94	2.50	3.00
Contacts	4.00	4.06	2.00	2.19
Photos	4.00	4.06	2.00	2.62
File Systems	4.00	4.31	1.50	1.75

Table 6. Privacy sensitivity and Access Comfort by permission type in non-Persons condition.

Permission	**Privacy Sensitivity**		**Access Comfort**	
	Median	**Mean**	**Median**	**Mean**
Calendar	4.00	4.00	3.00	3.19
Contacts	4.50	4.38	2.00	2.44
Photos	5.00	4.62	2.50	2.75
File Systems	5.00	4.44	2.00	2.25

4.4 Concern of Thomas's Privacy from the Lens of his Friends (RQ4)

The final research question addresses the scenario where participants are asked to assume they are Thomas's friend and are aware that the app has access to Thomas's sensitive data. This question examines their intent to install the app under these circumstances. The median and mean scores related to this question are summarized in Table 7 for all the four app permissions and both the persons and non-persons conditions.

In the non-persons condition, participants were reluctant for Thomas' friends to install the app which included app permissions such as file system, calendar, and photos; while in the persons conditions their intent to install prioritized app permissions such as calendar, file systems and contacts. These results aligned with the participants views on the intent to install applications from their own perspective, with file system ranking the lowest (mean = 1.25 vs mean = 1.50) and contacts ranking the highest (mean = 2.67, vs mean = 2.50) in the non-persons condition. However, in the persons condition, there was a significant difference between the intent to install an app with all the permissions across both the perspectives.

Table 7. Median and Mean scores that Thomas would be intent to install the app from the perspective of his friends on a 5-point likert scale, with lower values indicating lower intent to install

Permission	Median		Mean	
	Non-persons	Persons	Non-persons	Persons
Calendar	2.00	1.00	1.67	1.00
Contacts	2.50	2.00	2.50	2.00
Photos	2.00	3.00	2.20	2.80
File Systems	1.50	2.00	1.50	1.67

On running ANOVA between the persons and non-persons conditions, we found no statistically significant differences between participants on this topic. However, on running ANOVA between different app permissions, we found statistically significant differences ($F = 5.797$, $p < 0.01$).

4.5 Demographics

Although the gender distribution in our study was particularly skewed, it was interesting to find that participants' opinions on the privacy of Thomas (Male: median = 4.0, mean = 3.793; Female: median = 4.0, mean = 4.0) and on the privacy of his friends (Male: median = 4.0, mean = 3.391; Female: median = 4.0, mean = 3.857) were largely similar. This contrasts with the findings presented by [16], where females expressed higher concerns about installing applications that requested permissions, with a median of 5.00.

Similar to the skewed gender distribution among our participants, the ethnicity distribution was also skewed, with the majority of participants identifying as Asian. Participants who identified as Asian (median = 4.0, mean = 3.588) and those identifying as both Asian and White/Caucasian (median = 3.0, mean = 3.0) exhibited lower median and mean values for concerns regarding the privacy of the parties involved, compared to Hispanics and those identifying as both Hispanic and White/Caucasian (median = 5.00, mean = 5.00). Notably, ethnic groups with a higher percentage of participants in our study had lower median and mean concerns about privacy, which may have influenced these results.

When it came to the operating system used by our participants, majority of our participants used either Android or iOS on their smartphones as their primary choice for mobile OS. While the mean and median scores for privacy concerns for Thomas himself were mostly the same across Android and iOS OS' (Android: mean = 3.883, median = 4.00; iOS: mean = 3.800, median = 4.00), there were slight differences in the way they viewed the privacy concern for friends of Thomas, with participants on iOS being more concerned about their privacy than participants on Android OS (Android: mean = 3.00, median = 3.00; iOS: mean = 3.48, median = 4.00). However, none of these were statistically significantly different.

Next, we found similar statistics on the number of applications installed (Mean = Males(97.35) vs 109.10), number of photos in gallery (Mean = Males(4093.545) vs 4056.1) and number of personal, family events in their calendar (Mean = Males(0.4782609) vs 0.7142) across both male and female participants, which was contrasting the findings from [16] where they found that female participants had a significantly higher number of photos on their smartphones (Mean = 1468 vs 1067, $W = 39016$, $p < 0.001$). Using ANOVA, none of the metrics were statistically significantly different.

5 Discussion and Implications

In our discussion, we introduce design considerations to support interdependent privacy and discuss the broader implications of our results, specifically in the context of network topology. We also tie/link each section below to relevant course materials. Keep in mind that we had low participation for this iteration of the study, as such it is challenging to generalize and draw definitive conclusions from the results. However, we compare and connect our findings to the course materials and existing literature.

We observed that our participants cared more about their privacy than others when granting permissions. This aligns with the results of Marsch et al. [16]. This shows that one's privacy comes first before others or individuals are aware that they are sharing other's data by making decisions for them. This is alarming as, from a class paper, we know that people typically ask others not to share private photos and other data as their primary means of defending their privacy [6].

For answering RQ4, we saw no significant changes in their expectations of others to protect their privacy. This was also seen in other works like [15], where the guests did expect to know everything about the smart home set and their privacy in other's homes. This shows that the individual thinks it is too much to expect everyone to care about others' privacy. However, we saw in the original study results that people expressed their concern if others did not respect their privacy when making such decisions (at the end of the study) [16].

5.1 Design considerations to support interdependent privacy

In this section, we discuss two design considerations for smartphone application permissions and operating systems, pulling from several class readings to strengthen their validity. Similar to the original study, we confirmed that individuals were more concerned about their own data being compromised than their friends. Furthermore, we found that users were more concerned regarding the privacy of photos and file-systems applications than they were about their contacts and calendars. As a result, the design consideration section for mobile applications is written with a focus on photos and file-system applications.

5.1.1 Give data sharers features that allow them to preserve others privacy. In one of the class readings, Hong et al. talk about the importance of understanding the relationship between data sharers and data observers [11]. We know from this reading that both data sharers' and data observers' needs must be fully supported to have a system that preserves group privacy. Supporting data sharers in the context of smartphone photo apps could be realized by having a feature that allows users to select just the photos of themselves when sharing their photos with other apps. Giving users the benefit of sharing their photos with a third party while also preserving the privacy of others. Such a system could be implemented in that the phone or app shares only photos that contain the owner of the phone and nobody else. A more extreme example, but an example that could be more user-friendly and reduce the workload of the data sharer, could be to automatically anonymize other people's faces and likenesses in all photos that are shared in smartphone apps, similar to what was proposed with Facebook image sharing as seen in [14] .Such designs could prove useful, specifically those that automate privacy preservation, as we know from one of the class readings that people are often unaware that they have data on their devices that undermine others privacy [6]. A trade off does exist where the user would need to trust the system that manages shared data, likewise this same system would have to preserve the privacy of the user.

5.1.2 Use nudging and conflict detection to prevent interdependent privacy breakdowns. Smartphone manufacturers and those that create their operating systems perhaps have the most opportunity to protect interdependent privacy as they

can create operating systems that ensure not only the privacy of the individual but also the privacy of the group. This section introduces nudging and conflict detection as a meaningful way that smartphone operating systems can protect interdependent privacy.

Smartphone operating systems can divide the permissions that have an interdependent nature to them as highly sensitive, detect potential conflicts and give the user warnings. We know from a class reading written by Patil et al. that conflict detection is needed to avert awkward social situations[18]. Additionally we know from one of the class readings that nudging is an effective tool to make individuals aware of potential privacy violations [2]. We propose a design consideration that combines these two ideas such that smartphone operating systems detect conflicts and notify users through nudges when they are potentially engaging in behavior that is to the detriment of others' privacy. Furthermore to better support nudging and conflict detection, operating system designers can build an enhanced information architecture to allow users to specify how their data stored on others' devices should be managed. This was inspired by the class readings on System Design, particularly Privacy by Design (PbD) [5]. The theory aims to include privacy in the system design process rather than an add-on to the process towards the end.

5.2 Implications and Future Work

In the main study, the authors listed participants' reactions once they realized the motivation of the study [16] and realized how much more attention they would pay to the privacy of others after participating in the study. Our study could be thought of as a way of creating awareness of the interdependency in privacy choices. In some ways, we could also say this is a social engineering problem that could potentially have a huge impact on social behaviors. In the digital age, social cues do not transform well, which could indicate to users the interdependent nature of the choices they make about privacy. This also correlates to the intangibility of technology, which lacks the ability to indicate inherent social cues that would otherwise be captured easily.

As a part of future work, we could use the play of interdependency in network topology and the strength of the bond to indicate the dependency factor between users on their privacy. This was inspired by the readings from Social Theories, where we saw that network topology plays a huge role in securing information. We could look into how much of each node in a network secures information about the other nodes. Although this could encode the dependency by making the interdependency between nodes more evident, it is hard to decode the reasoning behind it and create awareness about it. For the reasoning, we thought of exploring a field study, which we learned during the week we discussed Research Methods. For future work, we can explore the same topic with other methods to identify more critical pain points of users who realize the interdependency.

6 Conclusion

Smartphones store increasingly more privacy-sensitive data related to other parties with whom users have personal or professional relationships. As a result, the choices made by individuals to share data on their phones impact others' privacy. To answer if individuals are aware of the interdependency in privacy when granting smartphone permissions, we conducted a survey with n=32 participants. We found that the participants were more concerned about their own privacy than others which could also be attributed to their unawareness. We propose changes to the privacy interfaces to indicate the interdependent nature along with the design of nudges and better system architecture to support users' needs to protect and respect other's privacy. In this way, it is important to look at privacy not just as an individual issue but as an interdependent and shared concern.

References

[1] Wael S Albayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. 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 446, 24 pages. https://doi.org/10.1145/3491102.3502097

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[3] Mary Jean Amon, Aaron Necaise, Nika Kartvelishvili, Aneka Williams, Yan Solihin, and Apu Kapadia. 2023. Modeling User Characteristics Associated with Interdependent Privacy Perceptions on Social Media. *ACM Trans. Comput.-Hum. Interact.* 30, 3, Article 40 (June 2023), 32 pages. https://doi.org/10.1145/3577014

[4] Hannah Brown, Katherine Lee, Fatemehsadat Mireshghallah, Reza Shokri, and Florian Tramèr. 2022. What Does it Mean for a Language Model to Preserve Privacy?. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (Seoul, Republic of Korea) *(FAccT '22)*. Association for Computing Machinery, New York, NY, USA, 2280–2292. https://doi.org/10.1145/3531146.3534642

[5] Ann Cavoukian. 2012. Privacy by Design and User Interfaces.

[6] Jason W. Clark, Peter Snyder, Damon McCoy, and Chris Kanich. 2015. "I Saw Images I Didn't Even Know I Had": Understanding User Perceptions of Cloud Storage Privacy. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1641–1644. https://doi.org/10.1145/2702123.2702535

[7] Kathryn D Coduto and Allison McDonald. 2024. "Delete it and Move On": Digital Management of Shared Sexual Content after a Breakup. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 918, 16 pages. https://doi.org/10.1145/3613904.3642722

[8] Antonella De Angeli, Mattia Falduti, Maria Menendez-Blanco, and Sergio Tessaris. 2023. Reporting non-consensual pornography: clarity, efficiency and distress. *Multimedia Tools Appl.* 82, 9 (Jan. 2023), 12829–12858. https://doi.org/10.1007/s11042-022-14291-z

[9] Mirko Franco, Ombretta Gaggi, and Claudio E. Palazzi. 2024. Characterizing Non-Consensual Intimate Image Abuse on Telegram Groups and Channels. In *Proceedings of the 4th International Workshop on Open Challenges in Online Social Networks* (Poznan, Poland) *(OASIS '24)*. Association for Computing Machinery, New York, NY, USA, 26–32. https://doi.org/10.1145/3677117.3685008

[10] Rakibul Hasan, Bennett I. Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your Photo is so Funny that I don't Mind Violating Your Privacy by Sharing it: Effects of Individual Humor Styles on Online Photo-sharing Behaviors. 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 556, 14 pages. https://doi.org/10.1145/3411764.3445258

[11] Jason I. Hong, Jennifer D. Ng, Scott Lederer, and James A. Landay. 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques* (Cambridge, MA, USA) *(DIS '04)*. Association for Computing Machinery, New York, NY, USA, 91–100. https://doi.org/10.1145/1013115.1013129

[12] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2020. A Survey on Interdependent Privacy. *ACM Comput. Surv.* 52, 6 (2020), 122:1–122:40. https://doi.org/10.1145/3360498

[13] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/Off: Preventing Privacy Leakage From Photos in Social Networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (Denver, Colorado, USA) *(CCS '15)*. Association for Computing Machinery, New York, NY, USA, 781–792. https://doi.org/10.1145/2810103.2813603

[14] Gan Liu, Xiongtao Sun, Yiran Li, Hui Li, Shuchang Zhao, Zhen Guo, and Yu-an Tan. 2023. An Automatic Privacy-Aware Framework for Text Data in Online Social Network Based on a Multi-Deep Learning Model. *Int. J. Intell. Syst.* 2023 (Jan. 2023), 23 pages. https://doi.org/10.1155/2023/1727285

[15] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM '20)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[16] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won't You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 437 (Oct. 2021), 35 pages. https://doi.org/10.1145/3479581

[17] Aaron Necaise, Tangila Islam Tanni, Aneka Williams, Yan Solihin, Apu Kapadia, and Mary Jean Amon. 2023. User Preferences for Interdependent Privacy Preservation Strategies in Social Media. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 271 (Oct. 2023), 30 pages. https://doi.org/10.1145/3610062

[18] Sameer Patil, Greg Norcie, Apu Kapadia, and Adam J. Lee. 2012. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 5, 15 pages. https://doi.org/10.1145/2335356.2335363

[19] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 104–124. https://doi.org/10.1145/3461778.3462040

[20] Kavous Salehzadeh Niksirat, Diana Korka, Hamza Harkous, Kévin Huguenin, and Mauro Cherubini. 2023. On the Potential of Mediation Chatbots for Mitigating Multiparty Privacy Conflicts - A Wizard-of-Oz Study. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1, Article 142 (April 2023), 33 pages. https://doi.org/10.1145/3579618

[21] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[22] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6777–6788. https://doi.org/10.1145/3025453.3025907

[23] Yuzi Yi, Nafei Zhu, Jingsha He, Anca Delia Jurcut, Xiangjun Ma, and Yehong Luo. 2023. A privacy-dependent condition-based privacy-preserving information sharing scheme in online social networks. *Comput. Commun.* 200, C (Feb. 2023), 149–160. https://doi.org/10.1016/j.comcom.2023.01.010

[24] Xiao Zhan, William Seymour, and Jose Such. 2024. Beyond Individual Concerns: Multi-user Privacy in Large Language Models. In *Proceedings of the 6th ACM Conference on Conversational User Interfaces* (Luxembourg, Luxembourg) *(CUI '24)*. Association for Computing Machinery, New York, NY, USA, Article 34, 6 pages. https://doi.org/10.1145/3640794.3665883

[25] Lotus Zhang, Abigale Stangl, Tanusree Sharma, Yu-Yun Tseng, Inan Xu, Danna Gurari, Yang Wang, and Leah Findlater. 2024. Designing Accessible Obfuscation Support for Blind Individuals' Visual Privacy Management. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 235, 19 pages. https://doi.org/10.1145/3613904.3642713

[26] Shiquan Zhang, Ying Ma, Le Fang, Hong Jia, Simon D'Alfonso, and Vassilis Kostakos. 2024. Enabling On-Device LLMs Personalization with Smartphone Sensing. In *Companion of the 2024 on ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Melbourne VIC, Australia) *(UbiComp '24)*. Association for Computing Machinery, New York, NY, USA, 186–190. https://doi.org/10.1145/3675094.3677545

A Questionnaire

A.1 Commitment

- We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in this study.
  Will you provide your best answers to each question in this study?
  - I will provide my best answers
  - I will not provide my best answers
  - I cannot promise either way
- What is your age (in years)? [dropdown of age from 1 to 120]
- What is the operating system of your primary mobile phone?
  - Android (Google)
  - iOS (Apple)
  - Windows
  - I do not know
  - Something else (please specify:) [text box]

A.2 Scenario Description

Imagine the following hypothetical scenario:

Thomas is an undergraduate student at his local University. He is looking for a new app for his smartphone. After some searching, he found an app which he installed on his phone without hesitation. This app asked for access to the [calendar OR contacts OR photos OR file system], which Thomas granted.

In the following, you can see a screenshot of his [calendar OR contacts OR photos] (See Figures 4,5,6,7,8,9, 10 and 11). Have a closer look at his [calendar OR contacts OR photos OR file system].

In the background, the application is sending the information stored in the [calendar OR contacts OR photos OR file system] to the server of the app maker.

[SCREENSHOT OF CALENDAR OR CONTACTS OR PHOTOS OR FILE SYSTEM, EITHER NON-PERSON OR PERSON]

A.3 Manipulation Check

- [MANIPULATION CHECK 1] What kind of [calendar events/contacts/photos] does Thomas have?
  Think of what you saw in the previous picture, and choose the correct answer.
  - CALENDAR:
    - Mainly listings of events (birthdays, parties, holidays, etc.)
    - Mainly listings of lectures
  - CONTACTS:
    - Mainly family and friends
    - Mainly companies and institutions
  - PHOTOS:
    - Mainly photos from family/friends/other people
    - Mainly photos from landscapes and cities
  - FILE SYSTEM:
    - Mainly files from family, friends, and others
    - Mainly files of lecture notes, landscape images, etc.

  [If the response is incorrect, show the participant the following text: The option you chose was wrong.
  CALENDAR: Thomas has mainly calendar events of [listings of events (birthdays, parties, holidays, etc.) / listings of lectures] on his phone.
  CONTACTS: Thomas has mainly contacts of [family and friends / companies and institutions] on his phone.
  PHOTOS: Thomas has mainly photos of [family, friends, and other people / landscapes and cities] on his phone.
  FILE SYSTEM: Thomas has mainly files of [lecture notes, landscape images, etc. /family, friends, and others] on his phone.]
- [MANIPULATION CHECK 2] What permission did the app ask for?
  - Access to Calendar
  - Access to Contacts
  - Access to Photos
  - Access to File system

  [If the response is incorrect, show the participant the following text: The option you chose was wrong.
  CALENDAR: The app asked for access to calendar.
  CONTACTS: The app asked for access to contacts.
  PHOTOS: The app asked for access to photos.
  FILE SYSTEM: The app asked for access to the file system.]

A.4 Interdependent Privacy

- Please indicate the extent to which you agree with each of the following statements: (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - Installing this app could jeopardize Thomas's privacy.
  - Installing this app would result in a high potential loss of privacy for Thomas.
  - Installing this app could lead to inappropriate use of Thomas's data.
- Please indicate the extent to which you agree with each of the following statements: (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - Installing this app could jeopardize the privacy of Thomas's friends.
  - Installing this app would result in a high potential loss of privacy for Thomas's friends.
  - Installing this app could lead to inappropriate use of Thomas friends' data.
- Please indicate the extent to which you agree with each of the following statements: (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - Thomas is responsible for protecting friends' data which is stored on his device.
  - Third parties are responsible for protecting friends' which is stored on Thomas's device.
- Assuming you were Thomas and knowing that this app has access to Thomas's [calendar OR contacts OR photos OR file system] (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - I would be willing to install this app.
  - It is likely that I would install this app.
- Assuming you were Thomas's friend and knew that this app has access to Thomas's [calendar OR contacts OR photos OR file system] (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - I would want Thomas to install this app.
- Assume again that you are Thomas. You have the chance to prevent access to your [calendar OR contacts OR photos OR file system] by using a paid version of the app instead of a free one. Both versions of the app provide the same functionality.
  What is the maximum amount of money you would be willing to spend in order to install the paid version of the app? [Text box]
- The following questions are NOT based on the scenario above:
  Please answer the questions from your own perspective. (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - Granting an app access to my calendar has the potential for revealing privacy-sensitive content.
  - Granting an app access to my contacts has the potential for revealing privacy-sensitive content.
  - Granting an app access to my photos has the potential for revealing privacy-sensitive content.
  - Granting an app access to my file system has the potential for revealing privacy-sensitive content.
  - I feel comfortable granting an app access to my calendar.
  - I feel comfortable granting an app access to my contacts.
  - I feel comfortable granting an app access to my photos.
  - I feel comfortable granting an app access to my file system.

- If an app asks to access calendar, contacts, photos and file systems, you cannot restrict access to only part of your calendar events, contacts, photos, or file systems. This app then has the possibility to read all of your calendar events, contacts, photos and file systems and transfer those to the server of a third party. Are you aware of this?
  - Yes
  - No

A.5 Smartphone usage

Please answer the following questions about your device usage.

- How many apps do you have installed on your phone at the moment? [INSTRUCTIONS AND SCREENSHOTS FOR HOW TO OBTAIN THE INFORMATION ON ANDROID AND iOS] [Text box]
- How many photos do you have on your phone? [INSTRUCTIONS AND SCREENSHOTS FOR HOW TO OBTAIN THE INFORMATION ON ANDROID AND iOS] [Text box]
- Did you approximate the number of photos?
  - I approximated the number of photos.
  - I gave the exact number of photos.
- How many contacts do you have on your phone? [INSTRUCTIONS AND SCREENSHOTS FOR HOW TO OBTAIN THE INFORMATION ON ANDROID AND iOS] [Text box]
- Did you approximate the number of contacts?
  - I approximated the number of contacts.
  - I gave the exact number of contacts.
- For a typical week, how many private/family-related calendar events do you have on your phone? [Text box]
- For a typical week, how many work/school-related calendar events do you have on your phone? [Text box]
- Please indicate your level of agreement with each of the following statements: (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - Companies today have the ability to place online advertisements that target you based on information collected about your web browsing behavior.
  - When you go to a website, it can collect information about you even if you do not register.
  - Popular search engine sites, such as Google, track the sites you come from and go to.
  - Many of the most popular third-party apps reveal users' information to other parties, such as advertising and Internet tracking companies.
  - I have recently helped a person with a problem.
  - I should go out of my way to help people more often.
  - If a member of my 'social group' comes to me with a personal problem, I'm willing to listen without being judgmental.
  - If a member of my 'social group' needs help on a task, I am willing to help even if it causes me some inconvenience.
  - I am willing to help a 'social group' member I don't know.
- Please be aware that the following questions are about your personal information. (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)

  - It usually bothers me when third-party app developers ask me for personal information.
  - When third-party app developers ask me for personal information, I sometimes think twice before providing it.
  - It bothers me to give my personal information to so many third-party app developers.
  - I'm concerned that third-party app developers are collecting too much personal information about me.
- Please be aware that the following questions are about personal information of your friends. (Options: Strongly Disagree, Somewhat Disagree, Neither agree nor disagree, Somewhat Agree, Strongly Agree)
  - It usually bothers me when third-party app developers ask me for my friends' personal information.
  - When third-party app developers ask me for my friends' personal information, I sometimes think twice before providing it.
  - It bothers me to give my friends' personal information to so many third-party app developers.
  - I'm concerned that third-party app developers are collecting too much personal information about my friends.

A.6 Demographics

Please tell us a bit about yourself.

- What is your gender?
  - ○ Woman
  - ○ Man
  - ○ Non-binary
  - ○ Prefer to self-describe: [text box]
  - ○ Something else (Please specify:) [text box]
- What is your ethnicity? (*Select all the apply*)
  - □ American Indian or Native American
  - □ Asian
  - □ Black or African American
  - □ Hispanic
  - □ Native Hawaiian or Other Pacific Islander
  - □ White / Caucasian
  - □ Something else (Please specify:) [text box]
  - □ Do not wish to specify
- What is the highest level of education you have completed? (If currently enrolled, highest degree received.)
  - ○ Less than High School
  - ○ Some High School
  - ○ High School Diploma
  - ○ Vocational training
  - ○ Some college but no degree
  - ○ College graduate (B.S., B.A., or other 4 year degree)
  - ○ Master's degree or Professional degree (e.g., Law, Medicine, Business, etc.)
  - ○ Doctoral degree

- Something else (Please specify:) [text box]

- What is your current annual household income?
  - Less than $10,000
  - $10,000 - $19,999
  - $20,000 - $29,999
  - $30,000 - $39,999
  - $40,000 - $49,999
  - $50,000 - $59,999
  - $60,000 - $69,999
  - $70,000 - $79,999
  - $80,000 - $89,999
  - $90,000 - $99,999
  - $100,000 - $149,999
  - More than $150,000
  - Do not wish to specify
- How long have you lived in the United States?
  - Less than 1 year
  - Between 1 year and 2 years
  - Between 2 years and 3 years
  - Between 3 years and 4 years
  - Between 4 years and 5 years
  - Between 5 years and 6 years
  - Between 6 years and 7 years
  - Between 7 years and 8 years
  - Between 8 years and 9 years
  - Between 9 years and 10 years
  - More than 10 years but NOT all of my life
  - All my life
  - I do not live in the United States
- What is the sum of three and four? [ATTENTION CHECK]
  - 4
  - 5
  - 6
  - 7
  - 8
- What is your year of birth?
  (dropdown of years from 1900 to 2023)
- What is / was your major field of study? [text box]
- What is your current relationship status?
  - Single, never married
  - Married

- Widowed
- Divorced
- Separated
- Something else (Please specify:) [text box]

- How many children do you have?
  - 0
  - 1
  - 2
  - 3
  - 4
  - More than 4
  - Do not wish to specify

B VISUAL DEPICTIONS USED IN THE STUDY

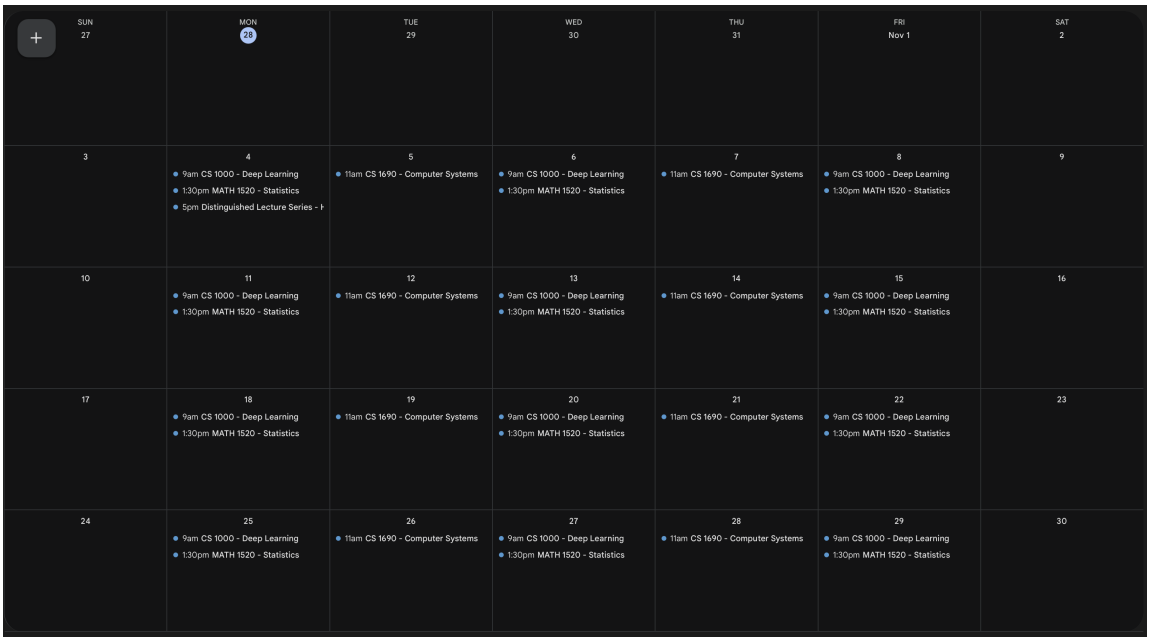


Fig. 4. Calendar visual depiction used in the Non-persons condition.

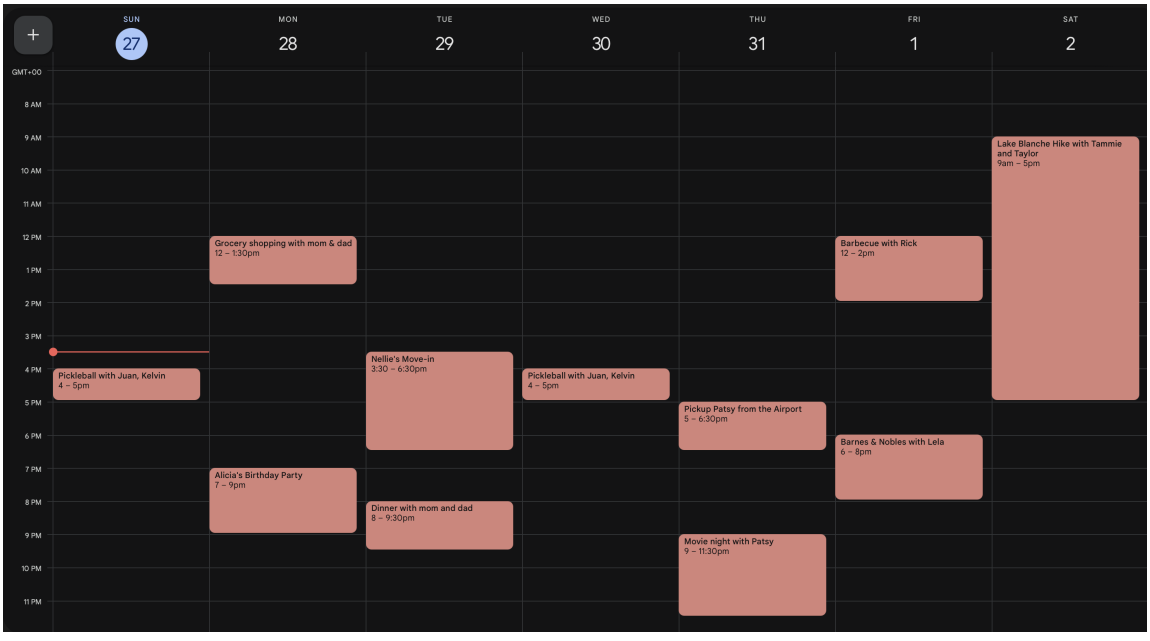
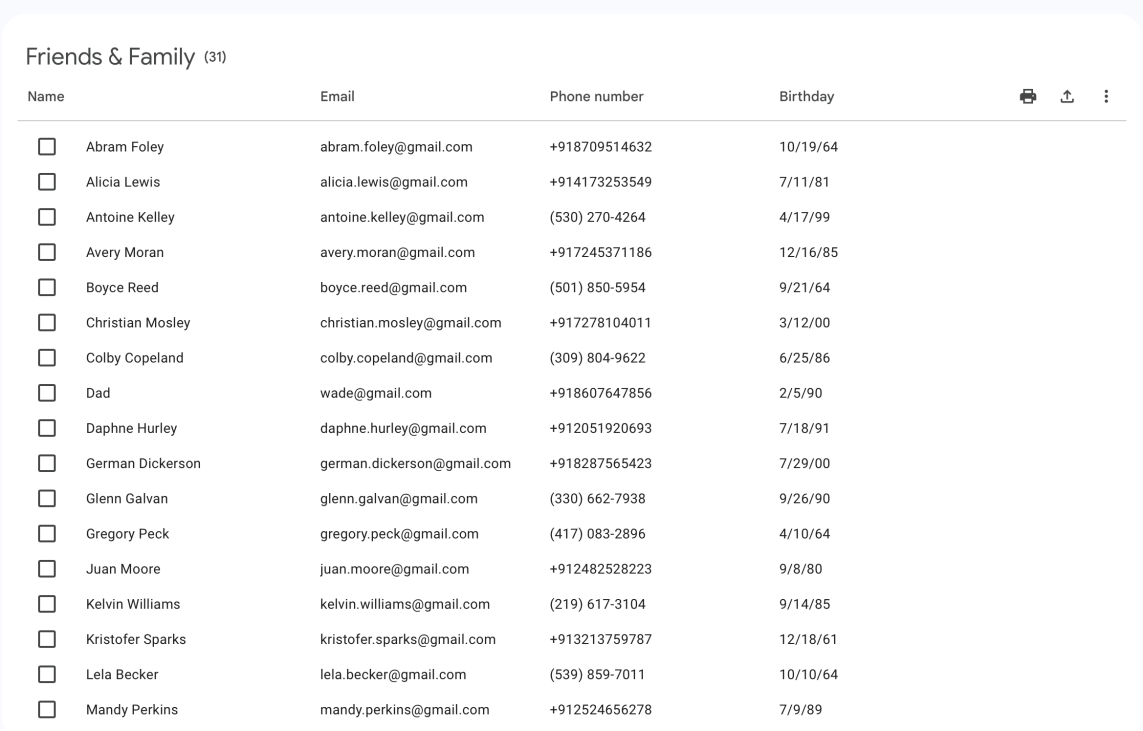


Fig. 5. Calendar visual depiction used in the Persons condition.

Organization & Services (25)

Name	Email	Phone number	Birthday
Campbell, Lewis and Smith	olarson@conway-lowe.com	+914762462718	
Carroll, Martin and Gray	gharper@contreras-moore.biz	431-137-0967x694	
Chandler Ltd	willislaura@greene.org	460-192-0975x217	
Clark, Ortiz and Roth	melissascott@rogers.com	+12563811913	
Davis-Durham	sheilaford@miller.com	+913605024179	
Graves, Davis and Smith	lisa97@flores-murray.com	+918890829902	
Hart PLC	williamsrobert@brock.net	(029)837-0645x645	
Herman, Henderson and Martin	macdonaldleonard@kerr.com	+12342346231	
Marshall, Wyatt and Chung	zlopez@ellis-wall.net	001-034-347-2750x596	
Martin, Smith and Allen	bullockbenjamin@johnson.biz	(408)477-8441x1524	
Miller Ltd	sandra69@williams.com	(287)613-2065x994	
Moore PLC	jwilliamson@neal.com	+916307096688	
Murphy, Preston and Edwards	christopher04@murphy.com	+918710639036	
Murray LLC	dannynorris@brown-sampson.org	+918733242730	
Nguyen-Simpson	john34@allen.info	+916360045238	
Nichols PLC	john55@roberts.info	+911939472733	
Nunez, Brown and Jackson	tmorgan@castillo.info	485-042-6869x49679	

Fig. 6. Contacts visual depiction used in the Non-Persons condition.



Friends & Family (31)

Name	Email	Phone number	Birthday
Abram Foley	abram.foley@gmail.com	+918709514632	10/19/64
Alicia Lewis	alicia.lewis@gmail.com	+914173253549	7/11/81
Antoine Kelley	antoine.kelley@gmail.com	(530) 270-4264	4/17/99
Avery Moran	avery.moran@gmail.com	+917245371186	12/16/85
Boyce Reed	boyce.reed@gmail.com	(501) 850-5954	9/21/64
Christian Mosley	christian.mosley@gmail.com	+917278104011	3/12/00
Colby Copeland	colby.copeland@gmail.com	(309) 804-9622	6/25/86
Dad	wade@gmail.com	+918607647856	2/5/90
Daphne Hurley	daphne.hurley@gmail.com	+912051920693	7/18/91
German Dickerson	german.dickerson@gmail.com	+918287565423	7/29/00
Glenn Galvan	glenn.galvan@gmail.com	(330) 662-7938	9/26/90
Gregory Peck	gregory.peck@gmail.com	(417) 083-2896	4/10/64
Juan Moore	juan.moore@gmail.com	+912482528223	9/8/80
Kelvin Williams	kelvin.williams@gmail.com	(219) 617-3104	9/14/85
Kristofer Sparks	kristofer.sparks@gmail.com	+913213759787	12/18/61
Lela Becker	lela.becker@gmail.com	(539) 859-7011	10/10/64
Mandy Perkins	mandy.perkins@gmail.com	+912524656278	7/9/89

Fig. 7. Contacts visual depiction used in the Non-Persons condition.

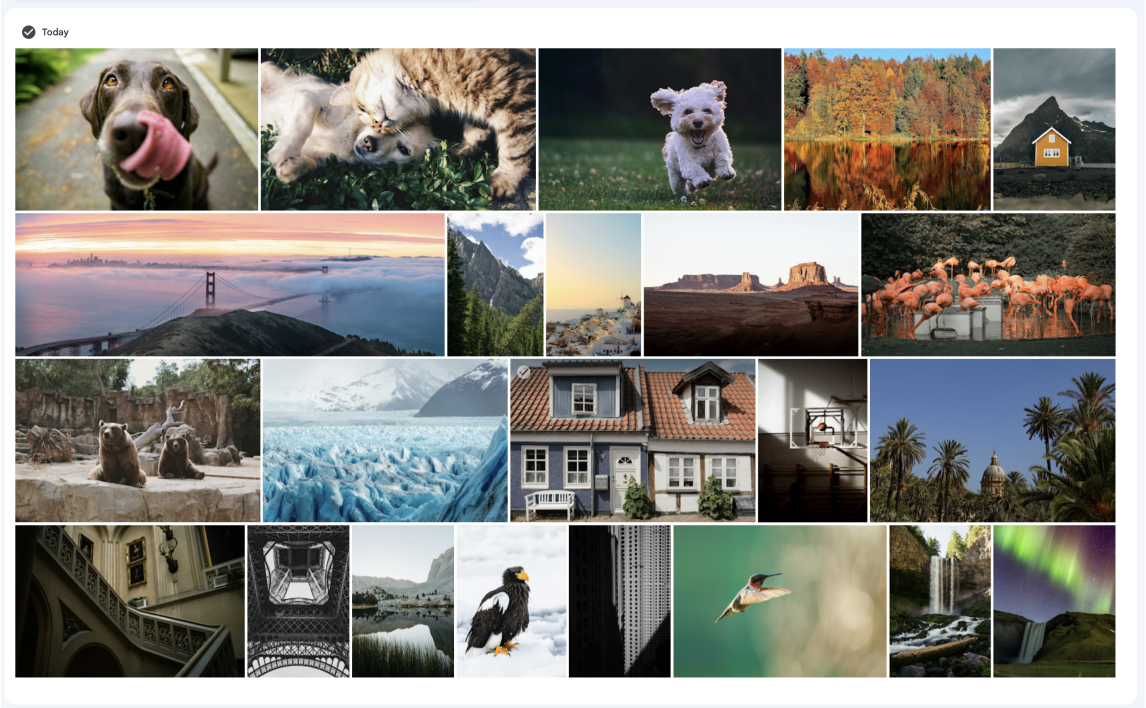


Fig. 8. Photos visual depiction used in the Non-Persons condition.

Fig. 9. Photos visual depiction used in the Persons condition.

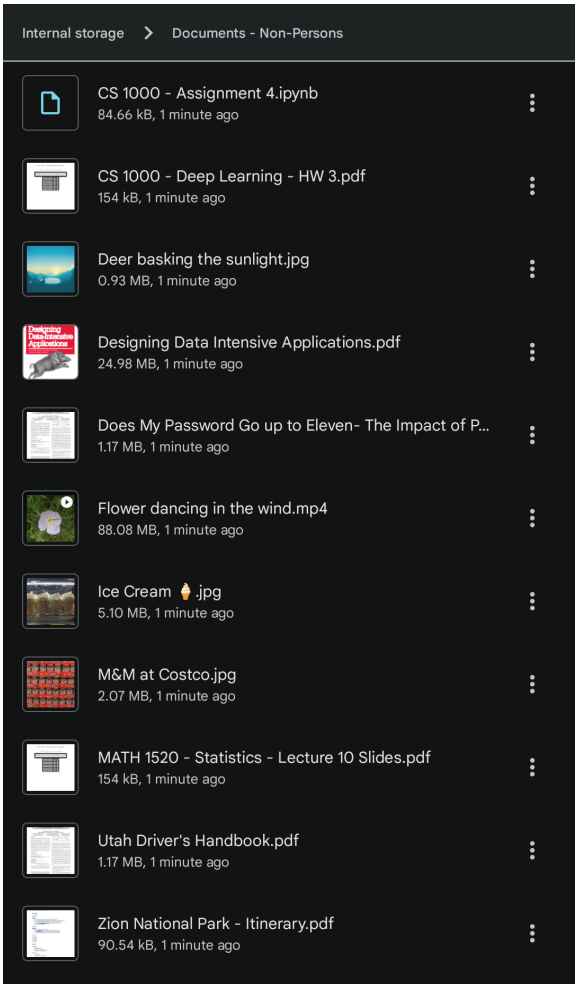


Fig. 10. File System visual depiction used in the Non-Persons condition.

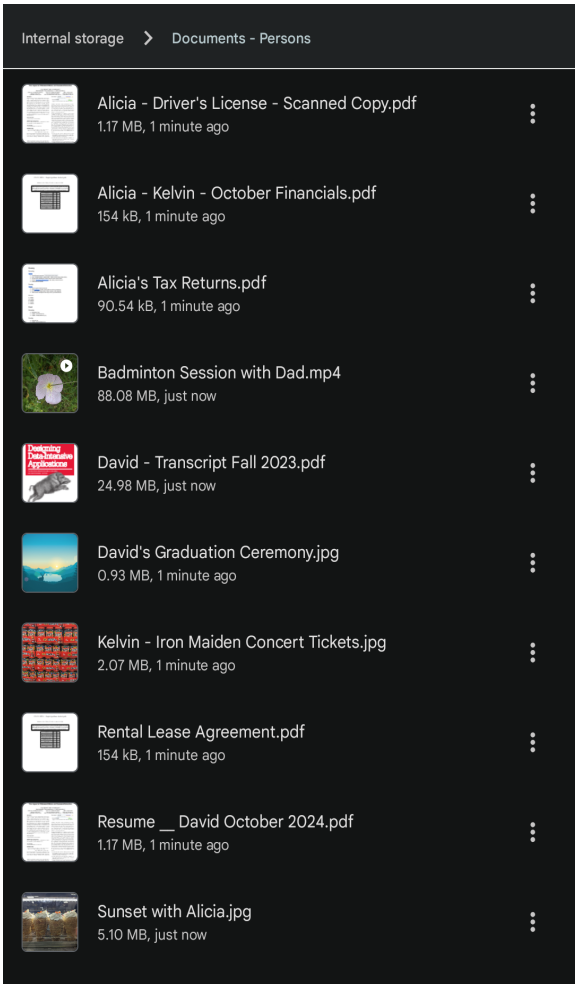


Fig. 11. File System visual depiction used in the Persons condition.

Received 20 February 2007; accepted 5 June 2009