Can I borrow your phone, again?

Clifford Bakalian
University of Maryland

Onur Cankur
University of Maryland

Emily Gong
University of Maryland

Justin Goodman
University of Maryland

Deepthi Raghunandan
University of Maryland

1 Introduction

Mobile phones have become a central part of modern daily life – 96% of Americans own a mobile phone [14]. Smart mobile phones, or smartphones, have also increased in popularity – 81% of Americans own a smartphone [14]. Among other basic functionality, like managing phone calls, smartphones have replaced the need for digital cameras, GPS systems, music players and even credit cards. These applications store enough data that personal privacy and security of smartphones has become a real consideration. More than one academic study has found there to be an imperfect solutions for protecting smartphones [7, 8] When we consider that smartphones are often shared, a behavior which was first explored in the paper, 'Can I borrow your phone?' [8], it becomes even more important to study and design security features people would be willing to use.

Karlson et al., and Matthews et al., found that, it is very common for smartphone users to share their devices, even though most smartphone users consider their phones as personal devices [8, 12]. Broadly, sharing behavior is often dictated by the trust in people with whom the device is shared. The level of trust is often dictated by the type of relationship between the sharer and the sharee. In addition, even this behavior can change based on the context in which sharing takes place. For example, regardless of the trust between people, sharing very personal data while in a public space still seems risky to most users. Modern smartphones have introduced different settings and modalities as a response to these findings.

Some smartphones allow 'guest' users to solely access application functionality, agnostic of personal data, without a password. For example, Samsung devices allow guest users to open the camera without providing access to previous photos[1]. Both Apple and Android smartphone devices allow for the 'pinned' application view which allow restricted use of a single app for guest users[2][3] Other phones also enable a multiple-login feature which allows the phone owners to actively manage data access.[4] Smartphones are also able to use context-aware security and privacy measures. For example, Android devices can impose locks based on users' locations.[5] In particular, users are asked if they would like to keep their phones unlocked while connected to their home wireless internet or while they are at their residence.

As we can see, smartphones have changed a lot since Karlson et al.'s study in 2008. Not only do smartphone hold more personal data, they also offer more ways of keeping data secure. We do not yet know whether these have affected sharing behavior among the average smartphone users. In this paper, we attempt to answer this question by replicating the study done by Karlson and team, with some key differences.

Both the original study and our are: observational in nature and done between subjects. Like Karlson et al., we measure how willing participants are to share their devices within different types of sharing relationships. We ensure that we can compare our results with those results of the original study, by asking survey participants about the similar relationships as those found in the original study. However, our study was done in a context in which lots of phone security are available and exist. Unlike in the original study, in which the authors conducted a semi-structured interview with 12 people from the Seattle area, we conducted a survey which reached more than 63 people from different areas in the United States. The goal of this decision was to reach a wider population and increase the rigor of our results. Our research contributions include: a list of survey questions

[1] https://www.samsung.com/uk/support/mobile-devices/what-is-private-mode-and-how-do-i-use-it/

[2] https://support.google.com/android/answer/9455138

[3] https://support.apple.com/en-us/HT202612

[4] https://support.google.com/nexus/answer/2865483

[5] https://support.google.com/pixelphone/answer/6093922

which can help to faithfully replicate the study done by Karlson et al., data from the study, stripped of personally identifiable information, and some key findings. We have gained some insight into how security features impact people's share habits and reaffirmed the findings of the original study that, smartphone users share differently within different relationships.

2 Related Work

Here we discuss three relevant areas of research pertaining to our study: phone security, user behavior with smartphones, and user profiles. In the phone security section, we discuss popular authentication schemes among smartphones of today and the direction of research in this area. In the user behavior section, we discuss research pertaining to users' perceptions of phone security settings. Lastly, in the profiles section, we discuss the research history around user profiles in smartphones. We tie some of these themes back to our research goals in this paper.

2.1 Phone Security

In 2019, 81% of Americans own a smartphone, up from 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011 [14]. As smartphone ownership has increased, improvements in phone security have developed right along with it. Previously, authentication schemes such as password/pin and patterns were popular methods. Biometric authentication such as fingerprint and facial authentication has become more popular in recent years [10, 20]. Most of these authentication schemes are common to the popular brands– iOS and Android. However, there are notable differences in some of the security features beyond authentication. Android users can limit access of some users to some applications, encrypt sensitive data, and include a wider variety of authentication methods [19]. However, the customization comes at a cost; the permission system relies on user's to make security decisions while the iOS permission model does not entirely depend on the users' decision [5]. **In this paper, we examine whether these design decisions make a difference in the way people share their phones**. However, even with the plethora of security features, some people are not aware of all the security features on their smartphones [9].

2.2 User Behavior

Some users may take precautions to defend their phone privacy, yet Redmiles et al. [16] explain how security advice is over-saturated and overwhelming. Alas, it is increasingly important to ensure, and research techniques for, smart-phone user security [1]. People often keep their phones unlocked or share devices for utility and convenience. Some users forgo device locking mechanisms for convenience of sharing with others. Although users find it a nuisance, many will lock for the benefits of security and privacy [6, 4]. Users motivate the locking mechanism through the protection of information on the phone and controlling the access from unwanted users (parents, kids, strangers, etc) [6, 4]. In [4], users motivate not locking the phone in situations where other users unlocking would be beneficial such as accidents or losing the phone. Users stated that they don't always want to lock out friends and other users but want to regulate the usage. Thus, the context of phone locking should consider the user's privacy preferences and the accessibility of the data stored through the device. In one of the closest works related to our study, [12], the researchers conducted a survey study, a diary study and several interviews about participants' devices, sharing experiences, and the reasons and motivations behind these experiences. The researchers state that users mostly share their phones with their significant others and their children. Additionally, they also state that users use fewer security features if they trust the person with whom they shared their device.

When concerning the risk perception of the mobile phone, users tend to underestimate the frequency at which they share their phone and the impact of the data from other users accessing their phone. In Engleman, many users reported finding social security numbers, credit/card debit cards, and other sensitive information stored in their email accounts. In addition, users saved the password for their primary emails within their phone which can be used to reset passwords. In [6], 52.7% of the participants were concerned about losing the phone and having to replace it while 11.9% were worried about account abuse and 8.8% were worried about data abuse. From this, we can see that security features may not matter if users do not care about them. **In our work, we examine whether users' concerns around security and privacy affect the way they share their phones**. We hope to motivate a security design which could fit the needs of smartphone users.

2.3 Profiles

One of the more promising security features for lending your phone is using profiles. Multiple 'profiles' (or spheres, or hats) would limit personal data and phone functionality based on different audiences or different contexts. Some literature specify a means to semi-automatically define profiles based on sensor data among others. These Implicit differentiation strategies include analyzing phone location [17], users' fingerprints, types

of touch, movement patterns [3], tapping patterns [13] and more.

Leading literature lays out a straightforward version of this strategy, an explicit means of differentiating context, in which users are encouraged to manually define different types of data access profiles ('spheres') based on different contexts [7, 15]. However, unlike Ni et al,, Hayashi et al. implement and study the viability of explicit differentiation of profiles at the OS layer and application layer. They introduce a way for users to configure a 'group account', within the OS, in which device owners can explicitly grant access to certain applications. They also develop a feature called 'activity lock' in which, via a button press, sharers can lock their phone to only provide access to one application to their guests. [7] find that users appreciated these features and suggested that they would use it in their real-life. [11], through xShare, introduce a file-level access specification which can be quickly and manually defined by users before sharing [11].

However, most of these strategies are employed to secure phones from unwanted users, and not necessarily switch the phone to a 'guest' profile. Work done by Seifer et al. is different [18]. Seifer et al. develop a semi-automatic means which restrict access based on device location and other sensor data. A study conducted in this paper finds that users feel more secure with such a privacy feature. However, the study fails to establish the viability of such a scheme for real-life scenarios. In particular, defining some security profiles took more than a minute for the average participant. Other bodies of work, [2] seem to suggest that profiles are not cost effective enough; in that, they are tedious to define manually, or even semi-automatically, and this cost is disproportionate to how little these features are used. We find the literature to be complete in this area and do not motivate our work to study the use of user profiles specifically.

3 Methodology

Our replication study was done with an intention to understand whether phone sharing behavior has changed since 2008. Thus, our research question contained two parts. We ask both *if* and *how* phone sharing behavior has changed. We also ask whether an increase in phone security features has changed phone sharing behavior. We developed our survey questions way to both replicate the original study and answer our research questions. In this section we will describe our methods for developing and distributing the survey (subsection 3.1), and analyzing our results (subsection 3.2). We also discuss limitations of our approach (subsection 3.3).

3.1 User Survey

Unlike the original paper, in which the researchers conducted an inductive interview study, we conducted a deductive observational survey study using a between-subjects design. This was done to increase the diversity and sample size of our study participants. However, in order to keep the survey as close to the original study as possible, we constructed most question to match that of the original study. To do this, we contacted the authors of the original study and obtained the script from their interview process.

As in the interview study, we asked how often respondents used 'basic phone functionality' like texting, calling and camera. We also asked respondents how often they share their phone within different, and common, relationships. These relationships could be mapped directly to the ones discussed in the original study so that we could eventually compare our results to the results found there. The survey also asks participants to categorize guest users based on how willing participants were to share their phones within these relationships. However, unlike in the original study, we asked about participants' usage of privacy/security settings and more specifically about settings found on both Android and iPhone devices. These questions were critical for us to better understand how the growth in phone security functionality has affected sharing behavior. We piloted the survey on each other as well as through the platform we later used. Using these statistics, we were able to estimate that the survey took approximately 10-minutes to complete. In total we asked 37 questions: 2 pre-screening questions, 16 questions regarding phone use, sharing, and security/privacy settings questions, 8 questions regarding demographics and 1 attention check. Please refer to Appendix A for a full list of questions.

We developed a recruitment and distribution plan once the questions were finalized. We planned to use Qualtrics[6] to create our survey and Prolific[7] to recruit participants and distribute the survey. Each participant would be: asked to consent to participating in the study, given an explanation of the purpose of the survey, and primed with an example of typical phone sharing behavior. We would only recruit participants who had a smartphone – ensuring this using a pre-screening question directly on Prolific. Using this plan, we obtained IRB approval to conduct the study. This allowed us to ensure that our plan was held to an ethical standard. There were no more than minimal risks in this study and participants had right to stop participating at any time and we protected their confidentiality by removing their Prolific IDs which was the only issue in this study that participant

[6] `https://umdsurvey.umd.edu`
[7] `https://www.prolific.co/`

might have concerns about.

3.2 Analysis

We obtained a total of 63 responses from participants on Prolific, within 20 minutes of initiating the survey on December 2020. The data was automatically collected by the Qualtrics platform and we downloaded that data in the form of a CSV. Each response was a row and each question component was a column in the CSV. After we obtained data, we decided to filter out respondents who did not pass our attention check. A total of 8 respondents said they were either slightly or very distracted while filling out the survey. We ultimately retained 55 responses for our final analysis.

When cleaning was done, we calculated a *permissiveness score* for each of the 10 sharing relationships which we had asked about in the survey. As in the original study, a permissiveness score is a number $\in [0, 1]$ which attempts to indicate how restrictive sharers are when allowing someone to borrow your phone. A permissiveness score of 1 indicates you would allow a guest group to access all parts of your phone, and 0 indicates the opposite. Our methods of calculation, however, diverged from the original study. Originally, the researchers calculated this permissiveness score by looking at the *access* the participant reported to have allowed per guest type per application. They then averaged the permissiveness score across all applications, within each relationship type, to obtain a permissiveness score for each relationship. In our approach, we directly asked the participant how permissive they were with their phone per sharing relationship [8]. We then normalized the likert values per guest type Figure 1 and averaged all scores to obtain an average score per guest-type.

To compare this data to the original study, we performed a hypothesis test. **Our null hypothesis was that there is no difference in permissiveness among guest-types in our data and the permissiveness among guest-types in the original data (H1).** We grouped the relationships to map directly to the 5 relationship types observed in the original study– family, friends, acquaintances, stranger and work associates. We mapped, parents/guardians, siblings, children, other family, and significant others directly to family. We mapped friend and roommate to the friend relationship found in the original study. Work associate, acquaintance and stranger relationships mapped one to one between our study and the original study. Once this mapping was complete, we compared the mean of mean permissiveness scores in each guest group from the original study to the mean permissiveness scores in each guest group from our study using an Krukal-Wallis test.

[8] Q9-11 in the survey

To determine which conditions could affect this permissiveness score, we grouped the participants into subgroups and took the normalized average permissiveness score per guest-type per sub-group. We used hypothesis tests to determined whether there there were difference between sub-groups. Sub-groups included: phone operating system, likelihood of applying security features, using their phone for work, level of phone usage and phone data plans. The subgroups regarding the phone's operating system and security were directly meant to help us test the effects of current phone security modalities on sharing behavior. Grouping respondents by those who used their phone, used their phone for work or had expensive phone plans was the way we tried to understand whether the level of utility derived from phones directly corresponded to permissiveness score. Note that plans were considered limited if any text, phone or data usage was limited by the respondents phone provider. All other groups formed based on multiple choice responses- each response was mapped to a number and later grouped using the numeric value.

- **(H2) There's no difference in permissiveness scores between Android and iPhone users.**
- **(H3) There's no difference in permissiveness scores between users who apply security setting to their phone and one who don't.**
- **(H4) There's no difference in permissiveness scores between users who use their phones for work and don't.**
- **(H5) There's no difference in permissiveness scores between users who use their phones a lot and don't use their phones a lot.**
- **(H6) There's no difference in permissiveness scores between users who have limited data plans and unlimited data plans.**

We tested each subgroup for normality and used either a one-way ANOVA test or Kruskal-Wallis test to detect differences between our subgroups. Since the groups were being tested multiple times, in a pair-wise fashion, we applied the bonferroni correction to our p-values. Our code is available on GitHub to encourage a reproduction of our results.[9]

3.3 Limitation

Since it is an observational self-report study, we needed to make sure that the participants were paying enough attention while answering the questions, so we added an attention check to mitigate it. The self-report nature of

[9] `https://github.com/jugoodma/can-borrow`

the may have caused a bias in our data. We may also see a slight shift in responses as there has been limited human contact for the past 9 months due to the COVID-19 pandemic. While we did offer example scenarios to help prime the participants, there is still the possibility that many forget what it's like for a stranger or acquaintance to ask to borrow your phone.

4 Results

In this section, we described our sample data and the results of our hypothesis tests. Hypotheses H2 and H3 help us test whether security changes and security design make a difference in how permissive users are in sharing their phones. Hypotheses H4, H5 and H6 help us test whether phone usage and reliance on phone functionality makes a difference in how permissive users are with their phones. H1 helps us test the permissive changes between the original paper and this study.

4.1 Sample Distribution

Our sample consists of 63 participants in total and 55 after the data cleaning. 32 of them were between 18-24 years old (58%), 20 of them were between 25-34 (36%), 2 of them were between 35-44 (4%), and 1 of them was older than 45 (2%). Also, 38 of our participants were male (69%), 16 of them were female (29%), and 1 of them had non-binary gender (2%). Their income was almost equally distributed with 17 participants that have less than $20,000 annual income (31%), 16 of them have $20,000-$49,999 (29%), 14 of them have $50,000-$99,999 (25%), and 8 of them preferred not to say (15%). In addition, 39 of the participants identified themselves as white (70%) but there were also some people who identified themselves as Hispanic, Spanish, or Latin (11 people, 20%), Asian (2 people, 4%), and 3 of them were unknown and preferred not to say. 39 of the participants have never married (70%), 7 of them are co-living with their partner (13%), 5 of them were married (9%) and the others preferred not to say. 18 of the participants have a bachelor's degree (33%), 12 of them have a high school degree (22%), 11 of them have some college degree (20%), and 7 of them have master's degree (13%).

Limitations As we can see, there are the limitation to using crowd-sourcing services, our sample is not very representative and generalizable. In addition to having lack of ethnic diversity, most of our participants are young, have low income and never married. Unfortunately, this limitation was inevitable for us due to lack of budget and time in this course project.

4.2 Sharing Relationships

We analyzed the permissiveness between different types of sharing-relationships in Table 1. For each guest type, we calculated a pairwise test. As a face validity, we checked if the three categories: 'definitely have concerns', 'some concerns' and 'no concerns', were statistically significant from each other. As expected there is a statistical significant difference between 'definitely have concerns' and 'no' and statistical difference between 'definitely have concerns' and 'some concerns' $p = 0.01$. It would be suspicious if there were similar levels of permissiveness given these categories.

Overall, participants rated sharing with strangers differently in comparison to every other group. Participants' permissiveness for 'Significant Others' was also statistically different than most other guest types except 'Parents' and 'Friends'. Based on the Figure 1, we can speculate that users are much more permissive with 'Significant Others' than 'Strangers', as one might expect. We tested whether permissiveness within these relationships were similar to those found in the original paper. We found that we could not reject the null hypothesis that these two dataset were the same, $p = 0.75$ (H1: Failed to Reject). See subsection 3.2 for details on the calculations.

4.3 Security

Users who applied security/privacy settings had statistically different permissiveness scores from users who did not apply settings, $p = 0.03$ (H3: Reject). However, we could not reject the null hypothesis that users with different OS had different permissiveness behavior, $p = 0.82$ (H2: Failed to Reject). Given the prior literature stating major differences for security features between OS [19], we would have expected a statically significant difference but our results do not support this.

4.4 Phone Usage

Participants who use their phones for less than one hour have a statistically different permissiveness scores than users who use their phone for more than 1 hour Table 2 $p = 0.0022$ (H5: Reject). However, there were only two users who use their phone for less than one hour and this subgroup did not have a 'normal' distribution. Participants who use their phone, in varying amounts, did not have statistically different permissiveness scores, (H4: Fail to Reject all scenarios). And lastly, we were not able to tell the difference in permissiveness behavior for phone users with limited data plans versus unlimited data plans $p = 0.64$ (H6: Fail to Reject).

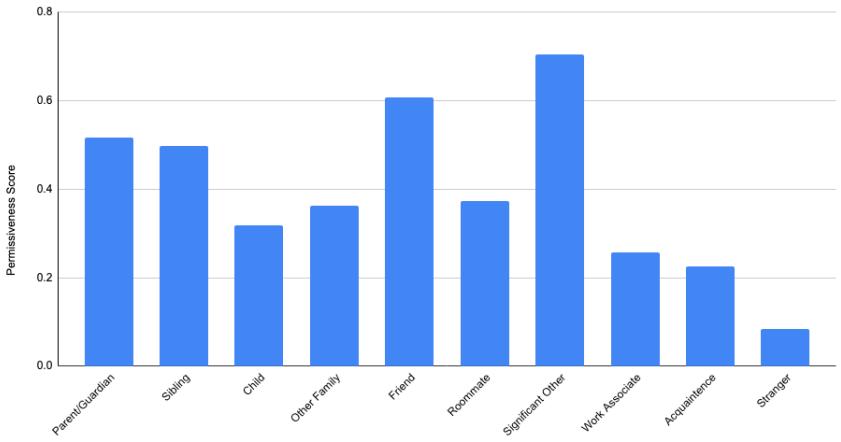


Figure 1: Permissiveness scores by guest type.

	Parents	Sibling	Child	Family	Friend	Roommate	Sig. Other	Work Assoc.	Acquaint.	Stranger
Parents										
Sibling	F									
Child	F	F								
Family	F	F	F							
Friend	F	F	**R**	**R**						
Roommate	F	F	F	F	**R**					
Sig. Other	F	**R**	**R**	**R**	F	**R**				
Work Assoc.	**R**	**R**	F	F	**R**	F	**R**			
Acquaint.	**R**	**R**	F	F	**R**	F	**R**	F		
Stranger	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	

Table 1: Results from pairwise test between relationships: F = failed to reject the null hypothesis, **R** = reject the null hypothesis ($p < .005$).

	$>$ 8 hrs	5-8 hrs	1-4 hrs	$<$ 1 hr
$>$ 8 hrs				
5-8 hrs	F			
1-4 hrs	F	F		
$<$ 1 hr	**R**	**R**	**R**	

Table 2: Results from pairwise test between phone usage levels: F = failed to reject the null hypothesis, **R** = reject the null hypothesis ($p < .0125$).

5 Discussion

Although phone functionality and security has developed in the past 10 years, there seems to be no detectable change in phone sharing behaviors within guest-types. However, there is a difference in phone sharing behaviors between people who use the security features on their phones and people who do not use them.

Due to budget and time constraints, we also decided to forgo asking questions about permissiveness per application and per phone function use-case, something the other study did. By asking application permissions, we could indirectly calculate a similar permissiveness score which could cut out some self-report bias. Additionally, we could have then potentially seen what apps and use-cases people are most hesitant to share. We leave the expanding of the study in this manner for future work. The other tasks that we leave for future work are providing a better definition of "permissive" in the survey, resolving key differences between OSes in terms of functionality and security features, and performing a semi-structured interview instead of survey.

We are also limited by the original study in terms of what we could compare our study to. The 2009 study, data on only 12 participants were collected [8]. Additionally, the data was collected via semi-structured interview, which due to time and pandemic constraints, we decided to replace with a online survey. Thus, we could not easily do a direct comparison between ourselves and [8]. Had we to do this study again, given more time and money, we would have performed semi-structured interviews and obtained more responses.

References

[1] ALSALEH, M., ALOMAR, N., AND ALARIFI, A. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one 12*, 3 (2017), e0173284.

[2] BRUSH, A. B., AND INKPEN, K. M. Yours, mine and ours? sharing and use of technology in domestic environments. In *International Conference on Ubiquitous Computing* (2007), Springer, pp. 109–126.

[3] DE LUCA, A., HANG, A., BRUDY, F., LINDNER, C., AND HUSSMANN, H. Touch me once and i know it's you! implicit authentication based on touch screen patterns. In *proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), pp. 987–996.

[4] EGELMAN, S., JAIN, S., PORTNOFF, R. S., LIAO, K., CONSOLVO, S., AND WAGNER, D. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014), pp. 750–761.

[5] GARG, H., CHOUDHURY, T., KUMAR, P., AND SABITHA, S. Comparison between significance of usability and security in hci. In *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)* (2017), IEEE, pp. 1–4.

[6] HARBACH, M., VON ZEZSCHWITZ, E., FICHTNER, A., DE LUCA, A., AND SMITH, M. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)* (2014), pp. 213–230.

[7] HAYASHI, E., RIVA, O., STRAUSS, K., BRUSH, A. B., AND SCHECHTER, S. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (2012), pp. 1–11.

[8] KARLSON, A. K., BRUSH, A. B., AND SCHECHTER, S. Can i borrow your phone? understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2009), CHI '09, Association for Computing Machinery, p. 1647–1650.

[9] KOWALSKI, S., AND GOLDSTEIN, M. Consumers' awareness of, attitudes towards and adoption of mobile phone security. In *20th International Symposium on Human Factors in Telecommunication* (2006), Citeseer, pp. 20–23.

[10] KUNDA, D., AND CHISHIMBA, M. A survey of android mobile phone authentication schemes. *Mobile Networks and Applications* (2018), 1–9.

[11] LIU, Y., RAHMATI, A., HUANG, Y., JANG, H., ZHONG, L., ZHANG, Y., AND ZHANG, S. xshare: supporting impromptu sharing of mobile phones. In *Proceedings of the 7th international conference on Mobile systems, applications, and services* (2009), pp. 15–28.

[12] MATTHEWS, T., LIAO, K., TURNER, A., BERKOVICH, M., REEDER, R., AND CONSOLVO, S. "she'll just grab any device that's closer": A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), CHI '16, Association for Computing Machinery, p. 5921–5932.

[13] MILUZZO, E., VARSHAVSKY, A., BALAKRISHNAN, S., AND CHOUDHURY, R. R. Tapprints: Your finger taps have fingerprints. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services* (New York, NY, USA, 2012), MobiSys '12, Association for Computing Machinery, p. 323–336.

[14] Mobile fact sheet, 2019. `https://www.pewresearch.org/internet/fact-sheet/mobile/`.

[15] NI, X., YANG, Z., BAI, X., CHAMPION, A. C., AND XUAN, D. Diffuser: Differentiated user access control on smartphones. In *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems* (2009), IEEE, pp. 1012–1017.

[16] REDMILES, E. M., WARFORD, N., JAYANTI, A., KONERU, A., KROSS, S., MORALES, M., STEVENS, R., AND MAZUREK, M. L. A comprehensive quality evaluation of security and privacy advice on the web. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (2020), pp. 89–108.

[17] SEIFERT, J., DE LUCA, A., CONRADI, B., AND HUSSMANN, H. Treasurephone: Context-sensitive user data protection on mobile phones. In *International Conference on Pervasive Computing* (2010), Springer, pp. 130–137.

[18] SEIFERT, J., DE LUCA, A., CONRADI, B., AND HUSSMANN, H. Treasurephone: Context-sensitive user data protection on mobile phones. In *Pervasive Computing* (Berlin, Heidelberg, 2010), P. Floréen, A. Krüger, and M. Spasojevic, Eds., Springer Berlin Heidelberg, pp. 130–137.

[19] SHABTAI, A., FLEDEL, Y., KANONOV, U., ELOVICI, Y., AND DOLEV, S. Google android: A state-of-the-art review of security mechanisms. *arXiv preprint arXiv:0912.5101* (2009).

[20] TEH, P. S., ZHANG, N., TEOH, A. B. J., AND CHEN, K. A survey on touch dynamics authentication in mobile devices. *Computers & Security 59* (2016), 210 – 235.

Survey Purpose

This purpose of this study is to understand modern smart-phone sharing habits. In general, the study wishes to understand how context and current phone capabilities influences how phones are shared.

Personal phones are ones you would use, primarily, to accomplish personal tasks such as: connecting with family and friends, or managing social media accounts which represent you. **This survey is asking you only about your personal-phone sharing habits.**

First, it will ask about how you use your phone to understand the data and features which are the most important to you. Second, it will ask about what you share the most often, who you share with, and how you felt about those experiences. Answer these questions to the best of your ability.
Third, the survey will ask about phone settings and applications which may have helped you share your phone and phone data more effectively. The survey will list possible categories of

people you share your phone with, and possible features you use on your phone.

Feel free to browse your phone and look at it for reference to ensure your answers are accurate.

The authors of this study will be removing any personally identifiable information, from the data collected here, before conducting analysis and using the results.

Scenarios

Example Scenario
The following scenario is an example of when a phone user might choose to share their phone or phone content. We hope that this scenario helps you remember your sharing experiences.

Onur was listening to music on his phone while he walked down the streets of his neighborhood to the corner shop. A young man, walking on foot, stopped him for directions to the closest department store. Onur, having never

frequented that part of town, pulled up the maps application on his phone to search for the store and guide the stranger. Onur unplugged his headset and handed his phone to the stranger to allow him to explore the map and find his way.

Example Scenario

The following scenario is an example of when a phone user might choose to share their phone or phone content. We hope that this scenario helps you remember your sharing experiences.

Deepthi and Cliff had found the perfect seats at the local movie theater. They had been instructed to save seats for their friends who were due to arrive shortly. Deepthi handed her phone to Cliff to coordinate their friends' arrival while she went out to get popcorn before the movie started.

Example Scenario

The following scenario is an example of when a phone user might choose to share their phone or phone content. We hope

that this scenario helps you remember your sharing experiences.

Cliff and Emily were on a road trip from San Francisco to Seattle. They took the wrong exit along the way and needed to find their way back to the right freeway. Emily was driving and Cliff was sitting in the front passenger seat next to her. Emily gave Cliff her phone password so he could unlock her phone and pull up the map application. Cliff used the map application to direct them to the right roads.

Example Scenario

The following scenario is an example of when a phone user might choose to share their phone or phone content. We hope that this scenario helps you remember your sharing experiences.

Emily was spending time with her close friend, Justin, at home. She remembered there was a funny video she wanted to show him, but her hands were full. She gave Justin her phone password, asked Justin to unlock her

phone and play the funny video on a video streaming app so both of them could watch it while she multi-tasked.

Check

Do you currently use at least one smartphone?

- ○ Yes
- ○ No, but I did in the past
- ○ No, never have

What kind of smartphone do use for personal tasks?

- ○ Apple device (eg: any iPhone)
- ○ Android device (eg: any Samsung, LG, Motorola, OnePlus, Pixel, etc)
- ○ Nokia
- ○ Blackberry
- ○ [ ] Other

phone use

How often do you use the following applications/services? For those applications/services you do not use, leave the answer blank.

	Hardly ever	Rarely	Sometimes	Often	Very often
Call/Video	○	○	○	○	○
Camera/Video Recording	○	○	○	○	○
Call Log	○	○	○	○	○
Messaging (SMS, Facebook Messenger, WeChat, Slack, Mattermost, etc)	○	○	○	○	○
Voicemail	○	○	○	○	○
Contacts	○	○	○	○	○
Email	○	○	○	○	○
Web Browsing	○	○	○	○	○
Web History	○	○	○	○	○
App History	○	○	○	○	○
Utilities (settings, weather, etc)	○	○	○	○	○
Alarm	○	○	○	○	○
Calendar	○	○	○	○	○
Tasks	○	○	○	○	○
Text Notes / Voice Memos	○	○	○	○	○

How much of your phone usage is work related?

None at all	A little	A moderate amount	A lot	A great deal
○	○	○	○	○

How many hours, on average, do you use your phone per day? Feel free to explore the settings on your phone to find this information. The latest Android and iOS devices will have this information readily available.

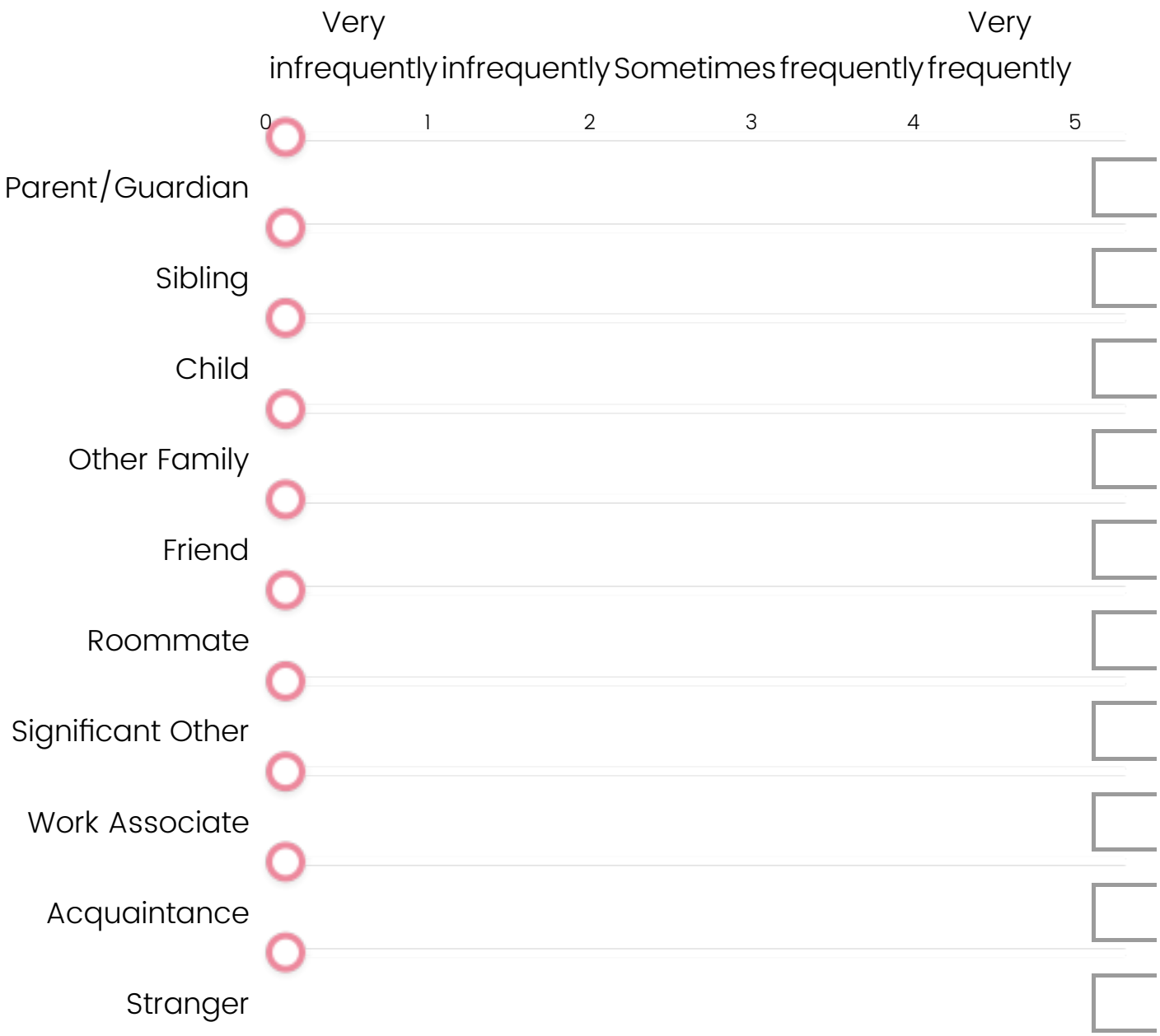
- ○ Less than 1 hour a day
- ○ 1 - 4 hours a day
- ○ 5 - 8 hours a day
- ○ More than 8 hours a day

phone sharing practices

Select each guest user type that you have shared your phone with.

- [ ] Parent/Guardian
- [ ] Sibling
- [ ] Child
- [ ] Other Family
- [ ] Friend
- [ ] Roommate
- [ ] Significant Other
- [ ] Work Associate
- [ ] Acquaintance
- [ ] Stranger

For each of the following guest user types, indicate how frequently you share your phone.



Group together the following guest user types which are similar. For relationships that you don't have, you may categorize as N/A

Items	Definitely have security and privacy concerns when sharing	Some security and privacy concerns when sharing
Parent/Guardian Sibling Child Other Family Friend Roommate		
Significant Other Work Associate Acquaintance Stranger	Definitely do not have security and privacy concerns when sharing	N/A

phone sharing practices (LM)

For the guests with whom you **${e://Field /Group1Name}**, indicate how permissive for the following access to your phone.

For the guests with whom you **${e://Field /Group2Name}**, indicate how permissive for the following access to your phone.

For the guests with whom you **${e://Field /Group3Name}**, indicate how permissive for the following access to your phone.

security

How long have you had a smartphone? (if you own more than one smartphone, answer in terms of your personal phone)

- ○ 0-2 years
- ○ more than 2 years, but less than 5 years
- ○ 5-10 years
- ○ more than 10 years

How many smartphones do you actively use?

- ○ 1
- ○ 2
- ○ 3
- ○ more than 3

How many tablets, or other mobile devices, do you have?

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ more than 3

What is your smartphone cellular plan?

	Limited	Unlimited
Phone Time (voice)	○	○
Text	○	○
Data Access	○	○

Do you apply settings on your smartphone to ensure privacy and security?

- ○ Yes
- ○ No
- ○ I don't know

What do you do on your smartphone to ensure privacy and security?

What security and privacy concerns do you have when sharing your phone?
Select all that apply.

- [ ] Physical integrity of the phone (it could get dropped and break)
- [ ] Personal data which you don't want to share
- [ ] Concerns that someone could change settings they don't know about
- [ ] Other concerns:

Are you aware that you can hide the content of your notifications from the lock screen? (Hide notification previews)

- ○ Yes, I use it
- ○ Yes, I don't use it
- ○ No

Are you aware that you can limit your phone to just the camera? (Guest mode)

- ○ Yes, I use it
- ○ Yes, I don't use it
- ○ No

Are you aware that you can prevent your phone from switching out of a chosen app, for example, locking your phone to a single app? (Screen pinning)

- ○ Yes, I use it
- ○ Yes, I don't use it
- ○ No

Does your phone have any security in regards to biometrics? (fingerprint, face ID, voice recognition, etc)

- ○ Yes, I use it
- ○ Yes, I don't use it
- ○ No

Are you aware that smart phones can come with 'smart lock' features? Some features include an ability to keep your phone unlocked while at home or while driving. Some phones can be locked automatically based on a timer.

- ○ Yes, I use it
- ○ Yes, I don't use it
- ○ No

demog

Demographics

What is your gender?

- ○ Woman
- ○ Man
- ○ Non-binary
- ○ Bi-gendered
- ○ No gender
- ○ [ ] Prefer to self describe
- ○ Prefer not to say

What is your age?

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55-64
- ○ 65 or older
- ○ Prefer not to say

What is your ethnic identity?

- ○ Hispanic, Spanish, or Latin
- ○ Native American Indian or Alaska Native
- ○ Asian
- ○ Black or African American
- ○ Native Hawaiian or Other Pacific Islander
- ○ White
- ○ Unknown
- ○ _____ Prefer to self describe
- ○ Prefer not to say

What is your marital status?

- ○ Married
- ○ Co-living
- ○ Widowed
- ○ Divorced
- ○ Separated
- ○ Never married
- ○ Prefer not to say

What is the highest degree or level of school you have completed?

- ○ Some high school
- ○ High school
- ○ Some college
- ○ Trade, technical, or vocational training
- ○ Associate's degree
- ○ Bachelor's degree
- ○ Master's degree
- ○ Professional degree or doctorate
- ○ Prefer not to say

What is your occupation?

What is your annual household income?

- ○ Less than $20,000
- ○ $20,000 to $49,999
- ○ $50,000 to $99,999
- ○ $100,000 to $249,999
- ○ Over $250,000
- ○ Prefer not to say

When people work on tasks, they are sometimes in situations that can be distracting. How distracted were you while completing this survey?

- ○ Not distracted at all
- ○ Somewhat distracted
- ○ Very distracted