Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones

Amy K. Karlson, A.J. Bernheim Brush, Stuart Schechter
Microsoft Research
One Microsoft Way, Redmond, WA 98052
{karlson, ajbrush, stus}@microsoft.com

ABSTRACT

Mobile phones are becoming increasingly personalized in terms of the data they store and the types of services they provide. At the same time, field studies have reported that there are a variety of situations in which it is natural for people to share their phones with others. However, most mobile phones support a binary security model that offers all-or-nothing access to the phone. We interviewed 12 smartphone users to explore how security and data privacy concerns affected their willingness to share their mobile phones. The diversity of guest user categorizations and associated security constraints expressed by the participants suggests the need for a security model richer than today's binary model.

Author Keywords

Mobile phone sharing, phone privacy, phone security.

ACM Classification Keywords

H.5.3 User Interface; user centered design.

INTRODUCTION

As mobile phones increasingly support users accessing data and running applications that were previously only available within the relative physical safety of homes and businesses, enabling users to secure their phone-resident data is becoming more important. However, today's phones still use a binary (locked/unlocked) security model designed over a decade ago when phones stored only call histories and contacts' names and numbers. This security model presupposes a single, primary user (the phone's owner) as is common in developed nations.

Yet there are a variety of common situations driven by convenience, social practice, or necessity that motivate users to share their phone with others, from giving a child the opportunity to speak to a distant relative to allowing a stranger to make an emergency call. In emerging markets, phone sharing has thrived as the practice has made mobile phone use economically viable for those who would otherwise be unable to afford to use them. Nokia has even targeted several new sharing-enabled phones for this market [1], with features that swap phonebooks and track costs on a per-user basis.

However, phone sharing is not limited to economic necessity. Weilenmann and Larsson [4] anonymously observed phone sharing behaviors among urban Swedish teens and found that many of their sharing practices were social in nature, such as collaborative calling and SMSing. Steenson and Donner's [3] findings from field interviews of urban Indian families highlight that despite presumptions about economic pressures, cultural factors can also influence phone sharing behaviors. For example, some wives had little interest in owning a phone that was distinct from their husband's.

Given prior studies' evidence of real-world phone sharing and the trends toward storing increasing amounts of personal and enterprise-sensitive data on phones, this data may be at an increasing risk of loss or exposure. We therefore sought to understand whether and how security and privacy concerns factor into current-day phone sharing practices. Unlike previous studies, which observed phone sharing practices, we actively engaged adult smartphone owners on issues of security and privacy. Furthermore, we focused on users in a market saturated by mobile phones.

We conducted semi-structured interviews with 12 smartphone users to explore why they shared their phones, who they shared with, and the concerns they had when sharing, or considering whether to share, their phones. We explored security and privacy concerns on two dimensions: the relationship between the phone's owner and the *guest user* with whom the phone was shared, and the functions and data that could potentially be accessed by the guest.

While we found that sharing was common, participants also expressed concerns and strong preferences about which data and functionality should be available to different categories of guest users. Because these preferences cannot be implemented under today's binary access control model, our results suggest that a richer security model is required to address concerns that cause people discomfort when sharing their phones with others. We draw upon our study results to offer design directions for new phone access models that better support sharing.

CHI 2009, April 4–9, 2009, Boston, MA, USA.
Copyright 2009 ACM 978-1-60558-246-7/09/04...$5.00.

USER STUDY

We conducted in-depth semi-structured interviews with twelve participants, each lasting about two hours.

Participant Profile

We recruited 6 male and 6 female smartphone users from the general population of the Puget Sound region who had shared their phone at least once with another person. We selected exactly half the participants of each gender (3) to be over—and under—a midpoint of thirty years of age, with an overall age range of 18-50 and a mean of 33.5. We recruited users of smartphones because these phones already support access to a wealth of personal and enterprise applications and data. People who do not use smartphones would not have experienced concerns over sharing as rich a set of resources. As features currently exclusive to smartphones make their way to lower-end devices, these security and privacy concerns will affect a growing proportion of the mobile phone market.

To ensure that we solicited opinions from a diverse set of people, we recruited participants who owned a variety of smartphones (Table 1) and worked in a range of jobs; they included a real estate agent, interior designer, UPS worker, college student, and general contractor.

Interviews

The interviews were structured into four phases:

Phone Use: Participants answered a questionnaire that gathered demographics and general phone use patterns, including the frequency with which they use nineteen common smartphone services and applications (e.g., phone calls, SMS, email, calendar, etc.).

Phone Sharing Practices: Next we interviewed each participant about their phone sharing history. Participants began by describing scenarios that immediately sprang to mind about times in which they had shared their phones with other individuals or groups. Then, to help trigger additional memories, we worked through a list of 18 guest user types (e.g., family members, friends, work associates, strangers) and asked questions of the form "have you ever shared your phone with a/your [guest relationship]?" Pilot interviews convinced us that this format helped people recall less frequent sharing episodes. We recorded data about the guest, the range of activities performed, the frequency of such sharing, and the participant's recollection of his or her comfort level while the guest was using the phone. As appropriate, we followed up with questions to clarify nuances related to the setting or social interaction.

Application and Data Sensitivity: We asked participants about their sensitivity around sharing data associated with each of the applications they reported using on their phone. We streamlined the process by asking participants to group together those guests for whom they had the same security and privacy concerns regarding sharing. We also asked participants to assign descriptive labels to each guest group (e.g., "family", "work") emphasizing that a group could be disassembled at a later point if it no longer seemed apt, which happened in one case. Table 1 lists participants' chosen group labels.

Participant	Gender, Age	Phone Type	# Data Types Used	# Guests	# Guest Grps	Guest Group Labels
1	M,37	Nokia N95	16	6	5	Wife; daughter; son; friend & coworker; baby
2	F,47	Treo 700w	15	5	3	Daughter; friend; acquaintance
3	F,50	Blackberry Pearl	19	8	5	Family & close friend; friend; careless; coworker; stranger
4	F,25	Ericsson 750	17	4	4	Boyfriend; brother; close friend; acquaintance
5	M,50	Treo 750	13	8	4	Family; friend; work associate; other
6	F,33	Samsung Blackjack I	19	6	4	Close friends and family; out of state family; low-tech family; stranger
7	F,22	HTC wizard	16	11	6	Friend; young entertainment; low-tech & uninterested; coworker; sister; acquaintance
8	M,25	iPhone	12	9	4	Friend; family; work; acquaintance
9	F,18	iPhone	17	6	3	Family; close friend; acquaintance
10	M,27	iPhone	17	7	5	Friend; girlfriend; coworker; parent; teen
11	M,45	Treo 755p	17	3	3	Wife; coworker; friend
12	M,23	Motorola Q	14	7	4	Girlfriend and family; friend; work; baby

For each application participants had reported using, we asked them to specify which actions (usually viewing, editing, deleting) they would choose to prohibit for each guest group. For example, we asked "If possible, would you want to prevent people in *your family* from *viewing email* on your phone?" We also asked whether their physical presence/absence would affect their desire to automatically prevent guest users from performing an action. For applications that maintain user state between sessions, we included questions about actions on that state (e.g., viewing call logs, deleting search history, etc.). To ground user responses in personal experience we asked participants only about data they used and people with whom they had a history of sharing. Our semi-structured format allowed us to explore nuances and exceptions that participants expressed.

Acceptance of New Security Models: Stajano [2] previously suggested that PDAs could benefit from having both public and private modes, or "hats", that would "draw a security perimeter" around private data when users were compelled to hand their device to another person. While Stajano focused primarily on implementation challenges, we used the final phase of our study to elicit participant reactions to a security model that restricted guests' access to data or services. For example, we asked participants their interest level in a phone that could enter a restricted mode (manually or automatically) when operated by a guest.

STUDY RESULTS

During the interviews, participants relayed to us details of 80 sharing relationships, which we summarize below.

Phone Sharing Practices

Given that we only required participants to have shared their phone with one other person to qualify for the study, we were surprised by how many guests participants reported sharing with. On average, participants shared their phones with 6.7 (μ=6.5, σ=2.2) different guest users, which they aggregated into an average of 4.1 (μ=4, σ=0.9) guest groups. Of the 80 total guests documented, 11% were romantic partners, 35% were non-spouse family members, 19% were work colleagues, 19% were acquaintances or strangers, and 16% were friends. Most participants were quite comfortable sharing their phones with others (82% of the time). Reasons cited in the 18% of cases where the owner was not comfortable included data privacy (e.g., P7:"I have a lot of personal information I don't want [my sister] to go into, like who I text message"), fear of data deletion (e.g., P2:"[my coworker] might delete something or mess something up"), carelessness (e.g., P10: "If I let [one of my parents] have [my phone] for a while they might set it down someplace and then I'd have to make them create a strategy to find the phone"), and confusing non-technical guests (e.g., P6 "[my mom] is not very tech savvy. If the phone rang or I got email I could imagine my mom going 'ah! what is this? what is it doing?'").

By far the most common reason for sharing one's phone was for making and receiving phone calls, which was reported for 50 of the 80 guests (63%). Phones were also shared for entertainment purposes such as web, games, music, and videos (30%), sharing features or content (24%), and photo taking and browsing (14%). Overall, sharing occurrences were sporadic, varying in frequency across participants as well as their guests. Only 4% of guests used participant phones on a daily basis. More often, sharing occurred weekly (24%), monthly (35%), or even less frequently (38%). The wide temporal distribution of sharing along with the fact that participants were nearly always present when sharing occurred (96% of the time), seems to suggest the behavior is fairly informal and spontaneous.

Application and Data Sensitivity

We analyzed participants' responses to questions about which actions they would prevent their guest groups from performing on each application or data type. One consistent response was that participants did not want any guest deleting any type of data from their phones.

For each application, we calculated a "permissiveness" score: the number of actions permitted for each guest group from among the set *run*/*view*, *add*, and *edit*. *View* was substituted for *run* for applications that inherently represent personal data (e.g., email, contacts, photos). For the web browser, we inquired about the browsing functionality (web-browsing) separately from the personal data associated with it (web-history). Under this policy, contacts had a maximum permissiveness score of 3 (view, add, edit) while the call log had a max score of 1 (view). For each participant and each of their guest groups, we assigned a permissiveness score for each application/data type by summing the number of permitted actions. Finally, to ensure that data types with larger scales were not over-represented in the data set, we normalized the scores to lie between 0 (no permission) and 1 (full permission), by dividing each by the max possible score for that data type.

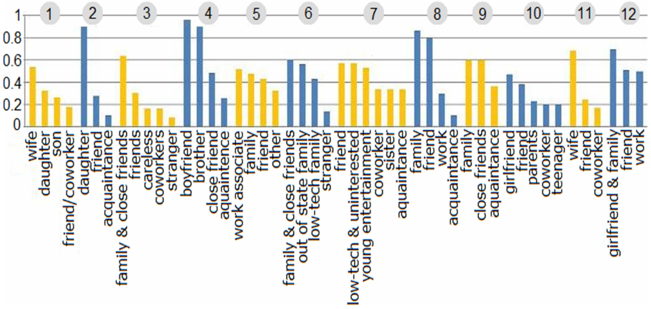

Figure 1. Average permissiveness scores for participants' guest groups (each color change marks a new participant).

Permissiveness by Group: For each guest group we calculated the average permissiveness score across all application/data types as a gross measure of the participant's trust in that guest group (higher scores indicate greater trust). The scores shown in Figure 1 highlight some interesting patterns. First, we notice that participants' permissiveness does vary across their guest groups, often showing one or two groups that have considerably more access than the others. Second, many participants give similar permissiveness scores to one or more of their groups (e.g., P7), suggesting that these groups might be equivalent when considering only application and data sensitivity. Finally, Figure 1 shows that permissiveness varies across participants; that is, some participants seem willing to give as much access to their low-permission groups as others give to their high-permission groups (e.g., P4 vs. P5).

Permissiveness by Application/Data Type: To derive a relative permissiveness ranking of the data types, we averaged each application/data type's permissiveness scores within and then across participant sharing groups. Based on this measure, we see from Figure 2 that most participants are comfortable letting others make calls and access photos, games, and the web (left-hand side). In contrast, participants were quite protective of applications that contained personal information, such as voicemail, notes, files, email, SMS, and calendars (right-hand side).

Presence: Our data suggest that presence is another factor that strongly influences comfort level during phone sharing. In 35% of the sharing scenarios described to us, the owner claimed that his or her discomfort would rise if the phone were out of sight. Out of 437 instances in which our participants said they would allow a guest group some degree of access to an application or data type, in 27% of those cases participants stated they would want the phone to

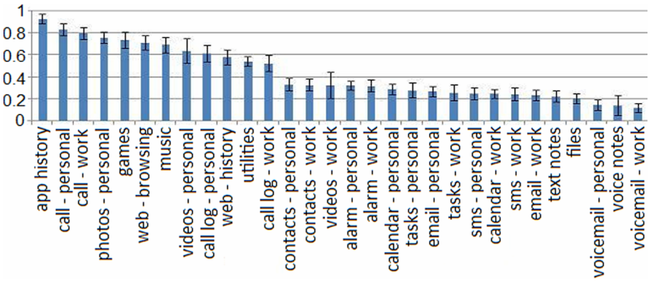

Figure 2. Average permissiveness by application/data type.

prevent access to that data or feature outside their presence. Data types for which presence mattered the most were videos (prevent access when not present in 7/8 instances), voicemail (7/12), SMS (9/18), contacts (10/26), and calls (19/43). However, if we consider only sharing with participants' single most trusted group (according to Figure 1) separately, not surprisingly presence seems to matter less. In only 18% of these cases would participants want to prevent access (vs. 32% of cases for their other groups).

Acceptance of Security Models that Assist in Sharing

All participants were in favor of a phone security model that could restrict access to data and services in some way when operated by a guest. Moreover, 9 out of 12 said they would want the phone to *automatically* enter a restricted mode if the phone could detect that the operator was a guest user. The fact that all participants agreed that the guest's access level would differ based on the owner' trust of the guest (μ=5, σ=0, on 5-point Likert scale) argues for phones supporting at least two levels of guest access. One solution that we proposed was the ability to set a guest "profile", analogous to setting a ring profile on today's phones; all participants found this to be a favorable candidate solution (μ=4.6, σ=.5). Under such a scheme, participants had a slight preference for profiles named according to the role of the guest (μ=4.7, σ=.7) as opposed to the activity the guest would perform (μ=4.2, σ=1.1), but generally thought either would be fine. Regardless, participants agreed any mode setting had to be fast (μ=5, σ=0) and easy (μ=4.7, σ=.5).

DISCUSSION

The ways in which our participants already share their phones as well as the differences in the access they would grant to their phone's applications and data across their guest groups suggest that better support for spontaneous sharing would be valuable on mobile phones. Furthermore, participants' levels of permissiveness across their guest groups indicate that 1-3 access settings might address much of the variation we found. Building interfaces that support the most restrictive use cases is likely the most valuable place to begin, since those were the events (e.g., loaning the phone to a stranger) that caused users the greatest concerns; they are also the times when the owner is most likely to make the effort to switch the phone to a restricted mode.

Evidence from the last phase of our study suggests that one approach would be to offer owners "guest profiles" that each restrict access to a subset of data or applications. But of course that is not the only possible implementation; another option would be to adjust the default boundary between public and private data so that low-sensitivity features like phone calls, games and web browsing are always assessable, while authentication would be required once phone operators try to access applications that expose personal information like email and calendar.

While some of the implementation options may seem reminiscent of user accounts on personal computers, or role-based access control, the design goal for phone sharing is a user experience that is intuitive and lightweight. We emphasize that switching to a restricted access mode should be more akin to changing one's phone ring type to "silent mode" than logging out and logging back into a computer. This is possible because the phone would have small number of guest profiles and authorizing the use of a profile can be simplified in the common case that the owner is nearby, even if her attention is elsewhere. For example, an owner could reasonably be expected to recite a PIN specific to a guest profile even if the guest user is responsible for entering it. Such easy transitions are not possible if phones must mimic multi-user PCs, where accounts for different users are protected by individual authentication processes. Note that mobile phone owners may not want to take conspicuous action to reduce a phone's permissions before giving it to a guest user because the guest may interpret this as distrust. Fortunately, phones can support commands to enter a lower-access state via inconspicuous input mechanisms such as gestures detected by motion sensors or buttons that lie under the owner's normal grasp.

CONCLUSION

Through our investigation, we have confirmed that the practice of phone sharing is not unique to teens or families in the developing world, but also extends to middle-class Americans, and as seen by others [3,4], is driven by a variety of social and pragmatic circumstances. We have also found that owner comfort level and permissiveness varies considerably according to the owner's relationship to the guest user, the type of activity for which a guest uses the phone, and the proximity of the guest to the owner. And finally, we noted that owners' comfort thresholds vary for different types of guests. These facts strongly suggest that today's all-or-nothing mobile phone security schemes are too coarse–grained and rigid to adequately meet users' security and privacy needs when sharing phones. We thus believe that changes in phone security models, for example enabling fast access to reduced-capability guest profiles, can make a valuable contribution toward addressing privacy and data integrity concerns during the common, but oft overlooked, practice of phone sharing.

REFERENCES

1. Nokia Inc. Nokia unveils two handsets that offer a range of useful features and colours aimed at consumers in emerging markets. Press Release (2007), http://www.nokia.com/A4805502.
2. Stajano, F. One user, many hats; and, sometimes, no hat–towards a secure yet usable PDA. *Security Protocols Workshop*, Springer Verlag (2004), 51-64.
3. Steenson, M. and Donner, J. Beyond the personal and private: Modes of mobile phone sharing in urban India. In S. W. Campbell & R. Ling (Eds.), *Mobile Comm. Research Annual (Vol. 1)*, Transaction Books (in press).
4. Weilenmann, A. and Larsson, C. Local use and sharing of mobile phones. In B. Brown, N. Green and R. Harper (Eds.), *Wireless World: Social and Interactional Aspects of the Mobile Age*, Springer Verlag (2001), 99-115.