Delphine Christin, Andreas Reinhardt, Matthias Hollick, Kai Trumpold: *Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications*. In: Proceedings of the 11th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM), pp. 14:1-14:10, December 2012.

Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications

Delphine Christin
TU Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany
delphine.christin@cased.de

Andreas Reinhardt
TU Darmstadt
Rundeturmstr. 10
64283 Darmstadt, Germany
andreas.reinhardt@kom.tu-darmstadt.de

Matthias Hollick
TU Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany
matthias.hollick@cased.de

Kai Trumpold
Goethe-Universität
Mertonstraße 17
60054 Frankfurt, Germany
trumpold@psych.uni-frankfurt.de

ABSTRACT

By leveraging smartphones as sensing platforms, mobile sensing applications can collect information in an unprecedented quantity and granularity. The transmission of unprocessed sensor readings can, however, pose severe threats to the users' privacy. To protect their privacy, users can apply filters to eliminate privacy-sensitive elements of the sensor readings prior to transmission. The resulting privacy protection depends on the configuration of these filters, which is controlled by the users through a privacy interface. In this paper, we study interface elements for the realization of this interface in order to foster its acceptance and maximize the efficacy of the provided privacy protection. To this end, we have implemented six graphical privacy interfaces, which have been evaluated by 80 participants of our user study. The results show a preference of the users towards differently colored and sized elements to visualize the current level of privacy protection and define their preferred privacy settings.

Categories and Subject Descriptors

H.1.2 [**Information Systems**]: User/Machine Systems—*Human factors*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; H.5.2 [**Information Systems**]: Information Interfaces and Presentation—*User Interfaces*.

General Terms

Design, Experimentation, Human Factors, Security.

Keywords

Privacy interfaces, mobile sensing applications, user study.

Copyright © 2012 by the Association for Computing Machinery, Inc. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Publications Dept, ACM Inc., fax +1 (212) 869-0481, or permissions@acm.org.

1. INTRODUCTION

The recent technological advances of mobile phones in terms of embedded sensors, storage resources, and processing capabilities have lead to the emergence of a plethora of mobile sensing applications. These applications rely on the mobile phones of voluntary citizens to collect sensor readings and monitor manifold phenomena. Example applications include the collection of sound samples for the construction of noise pollution maps [17], or analyses of the road quality based on accelerometer readings [15]. As the volunteers carry their phones in versatile places, the applications benefit from an unprecedented coverage. Simultaneously, the deployment costs are reduced to virtually zero compared to prior existing sensing solutions. However, most of current applications rely on the collection of data about the volunteers' environment, annotated with spatiotemporal information [5]. This collection of information about the users entails the risk of intrusions into their privacy by both the providers of the sensing application and other users of the system. Potential privacy threats may, however, hinder users from contributing to the applications, endangering the viability of the applications and thus, lowering their benefits to the community.

In the current state-of-the-art, a large majority of mechanisms specially tailored for mobile sensing applications concentrate on providing technically sound privacy-preserving solutions without taking the users into consideration [5]. Research results from orthogonal domains have, however, demonstrated that adopting this attitude mostly leads to either an inefficient application of the mechanisms supposed to protect the users or even their non-utilization by the users. For example, it was demonstrated that most users keep written copies of their passwords and thus reduce the efficacy of password-based authentication mechanisms [3] and do not protect their email transmission due to the complexity of the involved security mechanisms [20]. In order to avoid these pitfalls, we study the usability of interfaces designed to configure privacy settings. These privacy interfaces are specially tailored to the requirements of mobile sensing applications and allow each user to select at which degree of granularity and to which user(s) the collected sensor readings should be released. Our contributions address the challenge of privacy management on mobile devices, and can be summarized as follows:

1. We have designed six privacy interfaces in total, two to select

The documents distributed by this server have been provided by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, not withstanding that they have offered their works here electronically. It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.

users and four to select the degrees of granularity at which data is being shared. Each interface applies different concepts and interface elements in order to reflect the spectrum of user interface elements for mobile applications. We have implemented a prototype implementation of each interface on Android Nexus S mobile phones.

2. We have compared and evaluated them by means of a user study involving 80 participants. Our evaluation focuses on the (1) intuitiveness, (2) comprehensiveness, (3) ease of use, and (4) acceptance of all interfaces.

The paper is organized as follows. We first summarize existing work, before introducing our application scenario and listing our design drivers. We then present our design decisions and the resulting interfaces. We discuss the modalities and findings of our user study. After highlighting potential extensions to our work, we make concluding remarks.

2. RELATED WORK

In recent years, privacy interfaces have attracted significant attention in a wide range of application domains. For example, interfaces for website privacy policies, peer-to-peer file sharing systems, or online social networks have been analyzed and evaluated by means of user studies in [6], [8], and [13], respectively. These studies focus on either existing interfaces such as in [8] or new concepts, e.g., the Privacy Bird introduced in [6] or the the audience-oriented view of profile information proposed in [13]. Compared to [6, 13], we also intend to provide novel intuitive and usable interface designs, specially catering for increased privacy awareness by, e.g., the use of colors or varying areas and heights to represent the different levels of privacy protection. We, however, address an application domain orthogonal to these work, namely mobile sensing applications. In this particular application domain, the number of existing user studies is limited, even though users are the key elements of such applications. Indeed, mobile sensing applications leverage the mobile phones of volunteers and hence depend on their contribution to the application. The current state-of-the-art includes two relevant studies. In [4], the authors analyze how the participants understand, select, and feel comfortable with different obfuscation methods to achieve location privacy, while the authors of [12] concentrate on exploring the privacy concerns of users having taken part in a mobile sensing application. Further studies, such as [19, 11], broaden the focus of the analysis of privacy concerns to scenarios in which users share mobile phones with others. To the best of our knowledge, we are therefore the first to have designed privacy interfaces specially tailored for mobile sensing applications and evaluated their prototype implementation using an extensive user study.

3. APPLICATION SCENARIO

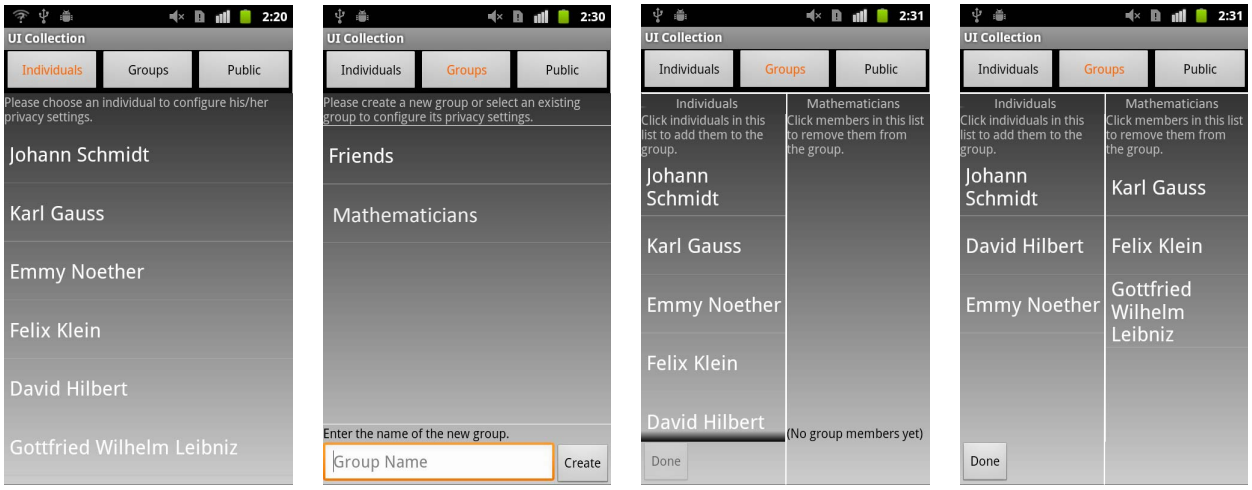
We assume a mobile sensing application, which collects data from the following sensing modalities using mobile phones: (1) location, (2) sound, (3) picture, and (4) acceleration. In absence of protection mechanisms, the collection of data from these sensing modalities poses threats to the user's privacy in several dimensions. Location data may reveal sensitive information about the users and their behaviors. For example, their political view may be inferred if the users attended political events, or their medical condition may be revealed by frequent visits to hospitals. Sound samples may capture private conversations about confidential and intimate subjects, and pictures may reveal the environments of the users. Moreover, acceleration data may be exploited to infer the current activity of the users or text sequences they entered on their mobile phone [16]. In order to protect their privacy, we assume that users collecting sensor readings can control the release of their data in two dimensions in order to protect their privacy. Firstly, they can decide to whom they want to release the data collected by each sensing modality. We assume that users can decide to share their collected sensor readings with particular individuals, groups of individuals, or to make them available publicly. Secondly, the degree of granularity at which the data is shared can be defined, as proposed in [7, 18]. Neither work, however, addresses how this paradigm should put into practice. For each sensing modality, the users can select one of the proposed degrees of granularity illustrated in Table 1. Note that the degrees of granularity chosen in the table can be easily modified without loss of generality. Starting with the finest granularity in the first row, i.e., the unprocessed raw data, the data resolution decreases until reaching the coarsest degree of granularity. Since the unprocessed data comprises the highest degree of detail, it can be expected to contain more privacy-sensitive information about the users. In other words, finer data reporting granularities pose more threats to user privacy. In order to realize the medium and coarse degrees of granularity, we assume that filters running on the user's mobile phone process the original sensor readings. For example, a filter eliminates the frequencies corresponding to human voice from the original sound sample, while another computes its loudness level [14, 17]. Additional filters are applied to blur faces present on pictures and count their number [1, 2], determine the user activity/position (between, e.g., sitting, walking, and lying) and whether he is moving based on original accelerometer data [9]. Despite the loss in granularity incurred by these filters, the application can still benefit from these data, even if they are coarse-grained. The design of these filters remains, however, out of scope of this paper.

Granularity degree	Location	Sound	Photo	Acceleration
Fine	Precise position	Original sample	Original image	Raw data
Medium	Street name	Voices removed	Faces blurred	Activity type
Coarse	City name	Loudness level	Number of people	Motion (yes/no)

Table 1: Selected degrees of granularity for the different sensing modalities

4. DESIGN DRIVERS

The primary objective of this work is to investigate the suitability of user interfaces specially designed for mobile phones in order to realize the aforementioned configuration of privacy settings. For convenience reason, the definition of privacy settings (i.e., the degree of granularity and the corresponding parties) is done directly on the devices that capture the sensor readings, i.e., the mobile phones. Using a secondary device, e.g., a computer, would unnecessarily increase the overhead for the users and may hinder them from modifying or updating their privacy settings; the efficiency of the privacy protection provided by the chosen approach would thus be limited. Consequently, the design of the user interfaces should take into account the constraints of the mobile phones in terms of layout and possible interactions. Since mobile phones offer a reduced screen compared to computers, we believe that the interfaces should be as *simple* as possible in order to outline the most important elements and facilitate their manipulation, while overloaded interfaces and complex interface hierarchies should be



(a) List of individuals (b) List of groups (c) Selection of individuals for the group “mathematicians" (d) Selected individuals in the group “mathematicians"

Figure 1: Selected screenshots of the list interface

avoided. Moreover, the interfaces should be *intuitive* and *easy to comprehend*, as extensive explanation cannot be supported due to the reduced screen space. We further assume that the interactions with the interfaces occur mainly through tactile elements. The elements of the interfaces should hence be *easily controllable* by potential users and the *number of required interactions* should be kept to a *minimum*. Finally, the interfaces should as much as possible help the users to understand the *implication of their choices* on their privacy. We focus on the prevalent user interface elements on current mobile phones, namely graphical interfaces, due to the multiplicity of privacy settings for the users to customize. Neither haptic interfaces, such as [10], that would require users to learn and control shaking patterns for each degree of granularity of each sensor modality, nor input methods based on audio, video, or textual input have been investigated.

5. DESIGNED PRIVACY INTERFACES

In this section, we present the interfaces we designed based on the above design drivers. The interfaces have been implemented for Android-based smartphones, more specifically the Google Nexus S. We first detail both alternatives to select users to share sensor readings with, namely the *list* interface (Figure 1) and the *spindle* interface (Figure 2). Both of these interfaces are extended by an additional interface allowing the users to select the degree of granularity at which the sensor readings are released to the selected users. For this interface, we have created four different alternatives explained below: the *phone* interface (Figure 3(a)), the *slider* interface (Figure 3(b)), the *radar* interface (Figure 3(c)), and the *bar* interface (Figure 3(d)). Note that all interfaces provide the same technical functionality, but present the configuration settings to the user in different ways. Therewith, we aim at exploring the preferences of the users in terms of design and interface elements.

5.1 Selection of Users

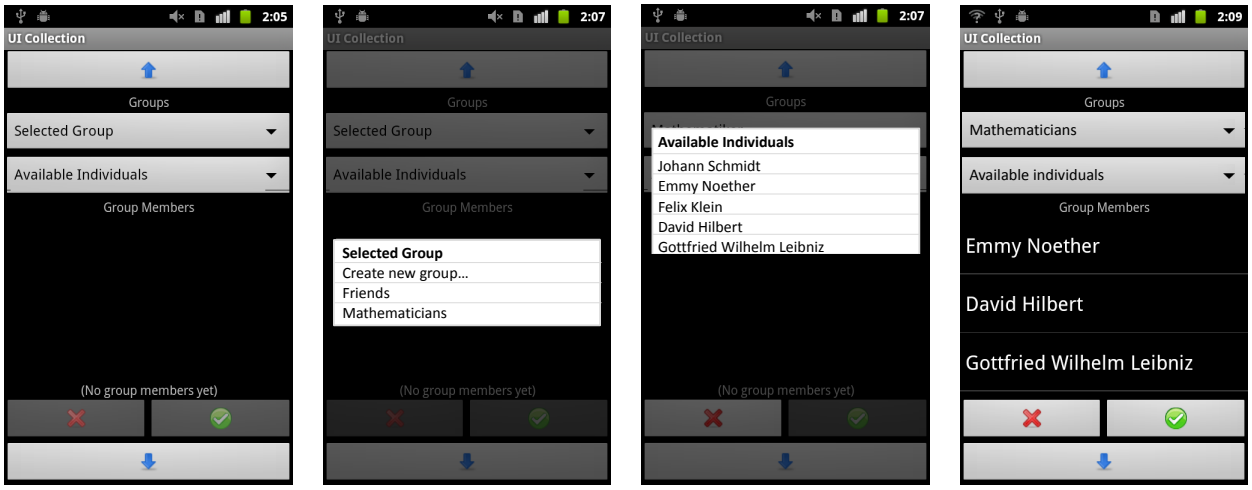
Using the list interface and the spindle interface, users manage who is able to access their sensor readings. They can select individuals, groups of individuals, or make them public. The *group* option allows users to simultaneously share sensor readings with the same degree of granularity with all individuals contained in the group. Users can create multiple groups, and add or remove individuals in each group.

5.1.1 The List Interface

The list interface illustrated in Figure 1 is based on three tabs located on top of the screen: *individuals*, *groups*, and *public*. The *individuals* tab leads to a list of individual's names (cf. Figure 1(a)). The list includes individuals belonging the social network of the user. Touching each name allows the user to individually select the degree of granularity for each sensing modality using one of the complementary interfaces presented below. Similarly, clicking on the *public* tab displays the same interface in order to select the degree of granularity to applied to the sensor readings made public. Under the *groups* tab illustrated in Figure 1(b), the user can manage existing groups, e.g., “friends" and “mathematicians", or create a new group by entering its name. After the group creation, the user can add new members to this group using the interface shown in Figure 1(c). The list on the left consists of individuals that can be added to the group, and the list on the right consists of the actual members of the group. Touching the names of individuals from the left list allows the user to add individuals to the group as represented in Figure 1(d). Touching members in the right list removes them from the group. Finally, when the *done* button is touched, the user proceeds to editing the degree of granularities for that group.

5.1.2 The Spindle Interface

Compared to the list interface, the navigation trough the spindle interface shown in Figure 2 is based on two arrows on the top and bottom sides of the screen. The arrows allow the user to navigate between the *individuals*, *groups*, and *public* categories. Instead of displaying all available individuals or groups, the spindle interface leverages spinners to save space and enables a direct integration of the interface for the configuration of the degree of granularity if possible. For managing the groups, the user accesses a unique panel shown in Figure 2(a), which presents two drop-down lists. The first list is used to create a new group or select an existing one as shown in Figure 2(b), whereas the second list contains available individuals to add to the selected group as shown in Figure 2(c). Touching a name automatically adds an individual to the current group. Figure 2(d) illustrates the members of the group “mathe-



(a) Group interface (b) List of groups (c) Selection of individuals for the group “mathematicians" (d) Selected individuals in the group “mathematicians"

Figure 2: Selected screenshots of the spindle interface

maticians". Touching the name of a group's member removes it from the group as in the list interface. Users can delete the selected group by using the red cross button at the bottom, or continue to the next interface for the selection of the degree of granularity by confirming the creation/update of the group using the button on the right. The structure of the spindle interface requires fewer interactions of the users when its function has been understood, since its function can be merged with the second interface for selecting the corresponding degree of granularity.

5.2 Selection of Degrees of Granularity

Once users have selected an individual, a group, or the public category using either the list interface or the spindle interface, they access a second interface in order to select at which degree of granularity they want to release their sensor readings to this particular party. To give the users a better overview over their current privacy settings, we have constrained the selection of the different degrees of granularity to a single screen. Moreover, the function to entirely disable the transmission of data from specific sensing modalities is also present in our prototype system, but is not part of the designed user interfaces.

5.2.1 The Phone Interface

The key idea behind the phone interface illustrated in Figure 3(a) is to reinforce the mental model of the users by showing the mobile phone at the center and the corresponding sensors at the periphery, since users are asked to select at which degree of granularity each sensor modality should be released. We use the image of a Google Nexus S phone, as the interface has been specially implemented for this platform. Users can change the selected degree of granularity by touching the pictogram associated to each sensor. The color of the pictogram depends on the current degree of granularity. The finer degree of granularity is mapped to red, the medium to yellow, and the coarser to green. In other words, red indicates that the privacy of the users may be threatened due to the selection of the finest degree of granularity, while green indicates a better privacy protection. A pop-up at the bottom of the screen recalls the name of the selected degree of granularity. Users can toggle through the degrees of granularity of each sensing modality by repeatedly touching the associated pictogram.

5.2.2 The Slider Interface

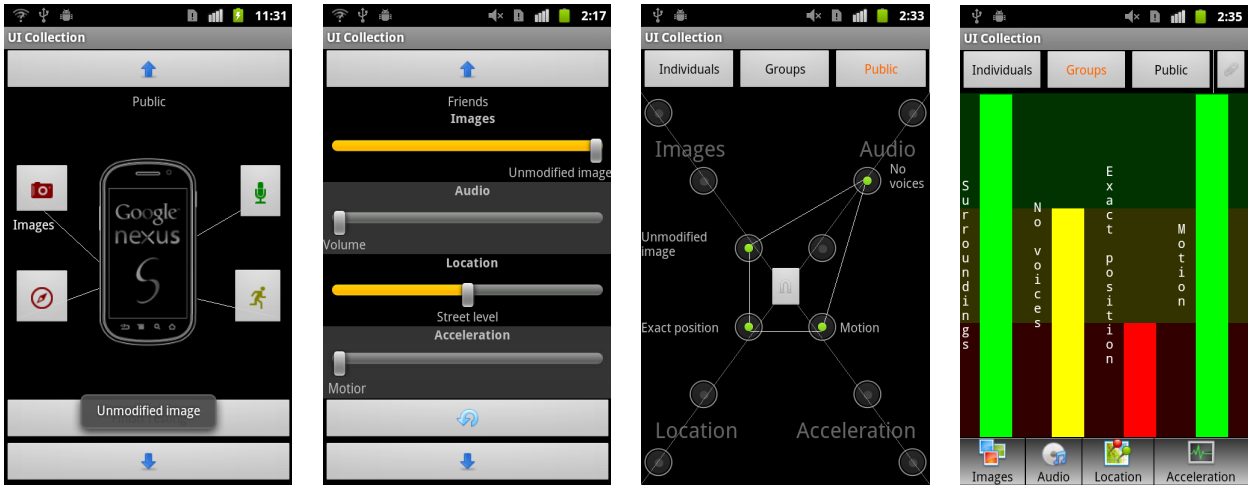
While the proposed degrees of granularity are discrete, we wanted to test an interface using sliders, which are a common and simple interface element. Additionally, they should help to visualize the associated degree of privacy protection through the length of the colored bar and the position of the slider. In the slider interface shown in Figure 3(b), sliders on the left and a full grey bar are associated to the finer granularity, while moving the sliders to the right increases the yellow fraction of the bar and should increase the attention of users to warn them from potential threats to privacy. The sliders are completed by a text field indicating the currently selected degree of granularity. The other degrees remain hidden, in order not to overload the interface.

5.2.3 The Radar Interface

The radar interface illustrated in Figure 3(c) is arranged along two diagonal lines. Each half diagonal is dedicated to a sensor modality and presents three radio buttons, one for each degree of granularity. Touching a radio button makes the name of the corresponding degree of granularity appear and selects it as current setting. The selected radio buttons are connected together in order to form a radar chart. The idea behind the radar chart is to illustrate the degree of privacy protection through the area of the formed shape. For our prototype implementation, we decided that the larger the quadrilateral, the better the privacy protection is. Note that the contrary can also be applied, if we consider that the center of the radar represents the user and the closer the quadrilateral, the less information is shared with outsiders and the better the privacy protection.

5.2.4 The Bar Interface

Figure 3(d) shows the bar interface, which contains four vertical bars modeling a histogram, one associated to each sensor modality and its respective pictogram. Touching a pictogram toggles through the different degrees of granularity of the corresponding sensor modality and changes both the height and the color of the associated vertical bar. Both the color and the height of the bars are intended to give users an indication on how their privacy is protected. High and green bars indicate a high level of privacy protection, whereas short and red bars indicate a lower level of privacy



(a) The phone interface (b) The slider interface (c) The radar interface (d) The bar interface

Figure 3: Selected screenshots of the designed interfaces for selecting the degree of granularity of the released sensor readings

protection.

For all interfaces that rely on color-coded indications of the level of privacy protection, the graphical visualization is supplemented by textual descriptions in order to assist color-blind persons. Note that the spectrum of possible interfaces is not limited to the aforementioned interfaces. We have specially selected these interfaces based on the diversity of their elements to cater to an extensive comparative evaluation in the next section.

6. EVALUATION OF THE DESIGNED PRIVACY INTERFACES

We have performed an empirical user study in order to compare the aforementioned interfaces and further analyze preferences of potential users. We have advertised our study by posting announcement on multiple student forums and internal mailing lists in different departments at our university. In total, 80 participants volunteered to test and evaluated our designed privacy interfaces. The participants were rewarded for their contribution with refreshments, no monetary remunerations were offered. In this section, we first present demographics about the participants and then, provide details about how we conducted our user study. We finally present the outcomes of this study.

6.1 Demographics and Mobile Phone Proficiency

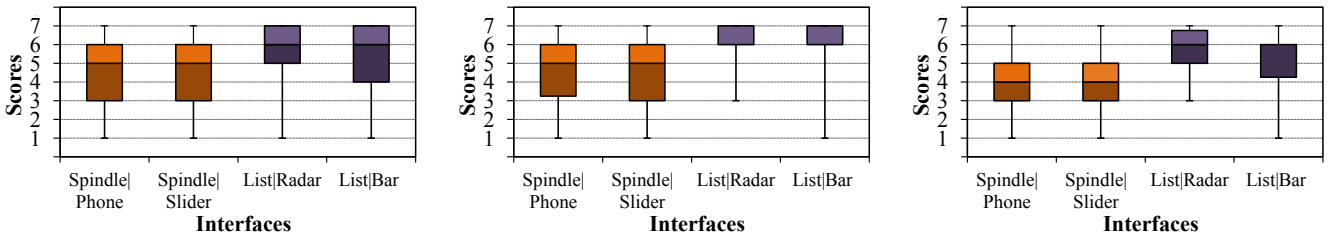
The participants of our study were predominantly male (n=56) and aged between 22 and 40 (m=28.6, SD=3.83). The group was composed of 20 undergraduate students, 41 graduate students, 4 postdoctoral researchers, 13 university employees, and 2 entrepreneurs. Their fields of occupation includes law, psychology, computer science, electrical engineering, mechanical engineering, and arts. While the participants present various profiles, they share common educational backgrounds and hence, may not be representative for all categories of the population. We have, however, specially targeted this category of people as they could be potential users of mobile sensing applications. Note that still 39% of our participants did not have any previous experiences with smartphones. Among the experienced participants, 37% were familiar with the Android operating system employed in our prototype implementation. The experienced participants were further asked to rate their estimated degree of experience with smartphones using a seven point Likert scale with a score of 1 for novice user and 7 for expert user. The results show that these participants think of themselves as relatively experienced (m=4.90, SD=1.45).

6.2 Evaluation Settings

For the evaluation, we performed the user study in the respective office environment of the participants under supervision. Each participant had one Nexus S phone configured with the set of the aforementioned interfaces and a counter invisible to the user, which counted the number of interactions for each interface element. In the experiment, both types of interfaces (selection of users as well as the degree of granularity) were being used. As these depend on each other, we have combined one interface of each type as follows. The list interface has been combined with both the radar and bar interface, while the spindle interface has been integrated into the phone and slider interfaces. Note that we have selected these combinations in order to limit the burden of the participants to the minimum, while offering the possibilities to the participants to compare different alternatives and hence, explore their preferences. Other combinations could, however, also be envisaged.

Additionally, each participant had a leaflet written in English including: (a) a brief introduction to mobile sensing applications highlighting the related privacy issues, (b) demographics questions, (c) instructions for the evaluation, i.e., the different tasks to solve using each interface, (d) a series of questions regarding each tested interface in terms of, e.g., ease of use, intuitiveness, speed, or appearance. The distributed leaflets included the instructions for testing and evaluating the interfaces in different orders in order to measure the effects caused by the order of presentation. Each participant successively tested all four proposed interfaces (combined with either the list interface or the spindle interface) by performing the same following set of tasks for each interface:

1. Create a group and define its privacy settings:
   (a) Create a new group with the name *Friends*
   (b) Add *Karl Gauss* to this new group
   (c) Define the privacy settings for this group as follows: original image, loudness level, street level, and activity type.



(a) "I find it easy to tell whether I am changing the settings for an individual, a group or the public"

(b) "Switching between individuals, groups or public is easy"

(c) "Managing groups and group members is intuitive and easy to understand"

Figure 4: Minimum, quartiles, and maximum score attributed to each statement in the evaluation of the list and spindle interfaces. A score of 1 indicates a strong disagreement and a score of 7 indicates a strong agreement.

2. Define the privacy settings for *Felix Klein* as follows: original image, original audio sample, precise position, and raw accelerometer data.

3. Set the *public* privacy settings in order to protect your privacy maximally.

The participants were able to ask the supervisor of the study in case of difficulties while testing and evaluating the full set of interfaces. In average, the completion of the study took approximately one hour per participant.

6.3 Evaluation Results

In this section, we first investigate the preferences of the participants between the list interface and the spindle interface. Next, we compare the answers of the participants specially regarding the phone, slider, radar, and bar interfaces. Additionally, we examine how the participants perceived the specificities of each interface.

We have preliminarily verified the independence of the answers of the participants on the order of the evaluated interfaces by means of a T-test for independent samples. The results show that the order of presentation of the interfaces does not significantly impact the answers of the participants. Moreover, further tests show that (1) the gender of the participants, (2) their experience in smartphones in general, (3) their experience in Android mobile phones in particular, do not significantly influence the answers of the participants. As a result, we subsequently present the overall results for the 80 participants.

6.3.1 *Comparison of the List and the Spindle Interfaces*

Since we proposed a combination of both interfaces to the users to test, we refer in the following as *List|Radar* and *List|Bar* to the list interface integrated in the radar and bar interface, respectively. Similarly, we refer as *Spindle|Phone* and *Spindle|Slider* to the spindle interface integrated in the phone and slider interface, respectively.

We first submitted the following statements to the participants in the aforementioned questionnaire: (a) "*I find it easy to tell whether I am changing the settings for an individual, a group or the public*", (b) "*Switching between individuals, groups or public is easy*", (c) "*Managing groups and group members is intuitive and easy to understand*". The participants rated this statement for each tested interface using a seven point Likert scale. A score of 1 indicates a strong disagreement, 4 is neutral, and 7 indicates a strong agreement. Figure 4 shows the minimum and the maximum scores attributed to the statements as well as the quartiles Q_1, Q_2, and Q_3. The results show a clear preference of the participants for list-style interfaces over the spindle type, with List|Radar obtaining the highest scores. These results are confirmed by the associated stanine scores presented in Table 2.

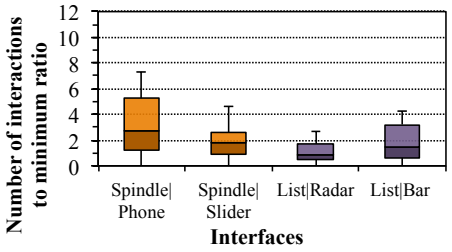


Figure 5: Ratio of the number of interactions compared to the expected minimal number of interactions for the list and spindle interfaces

Across all answers, the participants feel that the list is best suited for the identification of the category concerned by the change of settings. Furthermore, it was perceived as easier to navigate through, as well as more intuitive and easier to understand than the spindle interface compared to all answers.

In a second step, we analyze how the answers provided by the participants correspond to their experience with the proposed list and spindle interfaces. For this purpose, we consider the number of interactions necessary for the participants to solve the tasks related to the selection of persons. The tasks include the creation of the group *Friends*, adding *Karl Gauss* to this group, selecting *Felix Klein* and the *public* category to later change the associated privacy settings. We compute the difference between the actual number of interactions required by the participants and the minimal number of interactions required to complete the tasks. We then divide the result by the minimum number of required interactions and present the resulting ratio in Figure 5. A ratio of 0 indicates that the participant has succeeded in completing the tasks using the minimal number of interactions possible. Note that two participants did not correctly/fully completed the required tasks and thus, their respective ratios have not been taken into consideration in the computation of the overall results presented in Figure 5. Since the participants were not aware of the monitoring of their interactions in order not to modify their natural behavior, the present ratios may not only include the interactions necessary to solve the tasks, but also supplementary interactions of the participants used to freely discover the provided functions without any attempt to directly solve the task at hand. Figure 5 illustrates the minimum and maximum ratios as well as the quartiles obtained. By comparing the medi-

	Spindle|Phone	Spindle|Slider	List|Radar	List|Bar
I find it easy to tell whether I am changing the settings for an individual, a group or the public	4.31	4.48	5.92	5.30
Switching between individuals, groups, or public is easy	4.11	3.92	6.06	5.90
Managing groups and group members intuitive and easy to understand	3.88	4.25	6.16	5.71

Table 2: Stanine scores computed for each statement submitted to the participants for the evaluation of the list and spindle interfaces

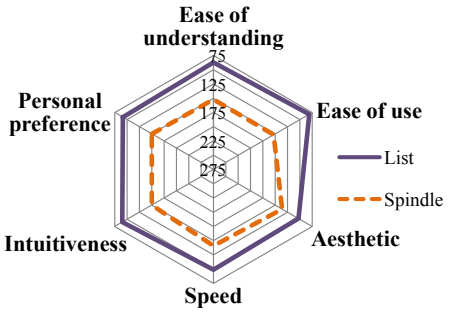


Figure 6: Cumulated scores obtained by the list and spindle interfaces. A score of 1 indicates the best interface and a score of 2 the worst interface in the ranking on the participants.

ans, the Spindle|Phone and Spindle|Slider interfaces globally require more interactions compared to the List|Radar and List|Bar interfaces. This result reflects the answers of the participants that highlighted the ease of use and intuitiveness of the list interface.

Next, we have asked the participants to rank the list and spindle interfaces with a score of 1 for the best interface and 2 for the worst interface according to following criteria: (1) ease of understanding, (2) ease of use, (3) aesthetics, (4) speed of use, (5) intuitiveness, and (6) personal preference. Figure 6 shows the cumulated score obtained by each interface for each criterion. Note that the lower the score, the more participants preferred the respective interface. We further asked them to comment on their ratings. The results show that the participants clearly preferred the list interface compared to the spindle interface. Some participants, however, particularly appreciated the aesthetics and speed of use of the spindle interface compared to the other criteria. A few participants specifically mentioned the advantage of the spindle interface over the list interface, e.g., "*no separate switching is necessary*" and "*less clicks are needed to manage the groups*". This however implies that the participants understand and memorize the structure of the interface, which is less visible than in the list interface. On contrary, some participants particularly appreciate the visibility of the options offered in the list interface: "*All choices are clearly visible*", "*Easy to find groups and individuals*", and "*All options at a glance, intuitive selection*".

In summary, the participants' answers and ratings as well as the initial number of interactions necessary for solving the tasks have demonstrated a large preference of the participants for the list interface, which appears to be simpler to control and more intuitive.

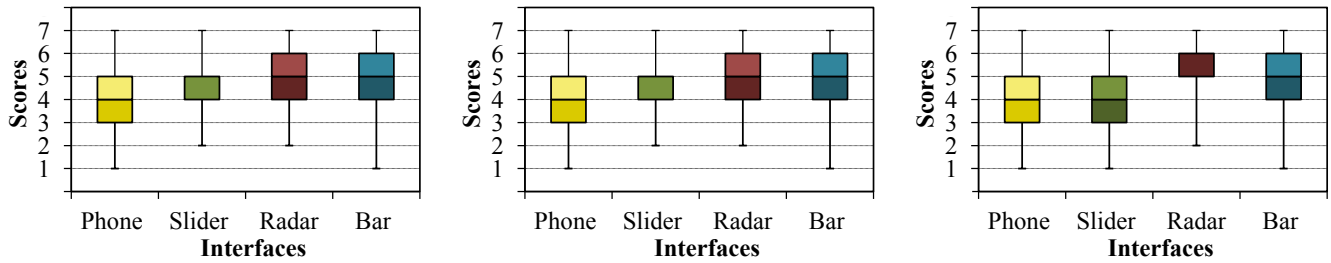
6.3.2 *Comparison of the Phone, Slider, Radar, and Bar Interfaces*

In this section, we concentrate on comparing the phone, slider, radar, and bar interfaces for selecting the appropriate degree of granularity of the each sensor modality. For this purpose, we firstly submitted to the participants the following statements to rate using a seven point Likert scale: (a) "*I find this interface intuitive*", (b) "*I find this interface easy to comprehend*", (c) "*I find this interface easy to control*", (d) "*I feel as if the data on the phone is being shared at a level I am comfortable with*", (e) "*I would accept this interface*", and (f) "*I would use this interface*". Figure 7 shows the minimum, the quartiles, and the maximum score attributed by the participants to each statement. A further analysis of the associated stanine scores presented in Table 3 confirms that the radar and bar interfaces are judged by the participants to be more intuitive, and easy to comprehend and control compared to the phone and slider interfaces. The participants also expressed stronger that using these interfaces the data on the phone is being shared at a level they are comfortable with. Additionally, they would be more ready to accept and use these interfaces than the phone and slider interfaces. By comparing the stanine scores for the radar and the bar interfaces, a slight preference of the participants for the radar interface can be identified, except for the statement "*I feel as if the data on the phone is being shared at a level I am comfortable with*".

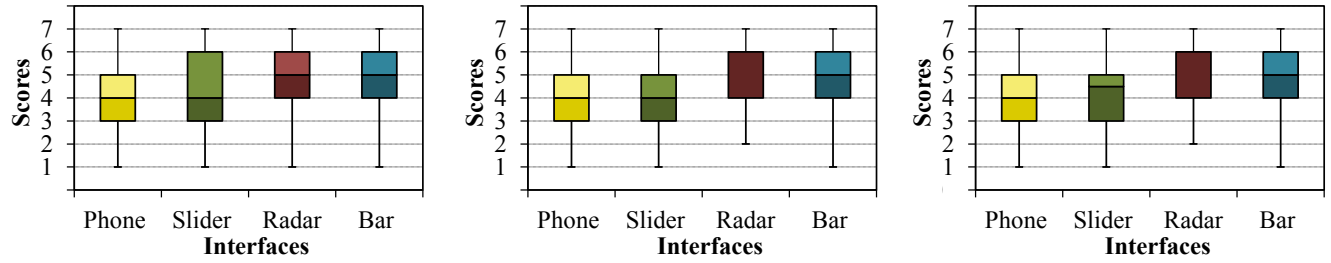
We compare in Figure 8 the number of interactions the participants required to configure the degree of granularity of each sensor modality according to the given tasks compared to the expected one. Using the bar interface globally required more interactions of the participants compared to the other interfaces. This difference may explain the the slight preference of the participants for the radar interface compared to the bar interface expressed in their answers. Moreover, the users require comparable numbers of interactions using the phone, slider, and radar interfaces. Overall, only few participants succeeded in completing the assigned tasks with the minimum number of interactions possible. This can be explained by the fact that the participants used the interfaces for the first time and were not familiar with them. Moreover, the participants had to follow given instructions that required them to switch between the mobile phone and the leaflet, potentially leading to errors that needed to be corrected later.

We next asked the participants to rank the phone, slider, radar, and bar interfaces, according to the same criteria as for the list and spindle interfaces using scores between 1 (best) and 4 (worst). Figure 9 represents the cumulated scores obtained for each interface. The lower the total score, the better the ranking. In general, the radar and the bar interfaces obtained better ranks compared to the other interfaces. The radar interface is judged by the participants to be easier to use, more aesthetic, and faster than the others. Additionally, a larger number of participants ranked it as their preferred interface. The rank for its intuitiveness is, however, close to that of the slider interface. In comparison, the bar interface is perceived to be the most intuitive and the easiest to understand. Between the phone and slider interfaces, the slider interface obtained better ranks, except for the criteria "ease of understanding" where the score is slightly greater than that of the phone interface. As a result, the radar interface obtained the best scores for four of the six criteria, confirming the preference of the participants for this interface.

We have finally investigated why the participants prefer one in-



(a) "I find this interface intuitive" (b) "I find this interface easy to comprehend" (c) "I find this interface easy to control"



(d) "I feel as if the data on the phone is being shared at a level I am comfortable with" (e) "I would accept this interface" (f) "I would use this interface"

Figure 7: Minimum, quartiles, and maximum score attributed to each statement in the evaluation of the phone, slider, radar, and bar interfaces

	Phone	Slider	Radar	Bar
I find this interface intuitive	3.83	5.09	5.80	5.28
I find this interface easy to comprehend	3.92	4.87	5.73	5.47
I find this interface easy to control	4.21	4.32	6.03	5.43
I feel as if the data on the phone is being shared at a level I am comfortable with	4.46	4.78	5.31	5.46
I would accept this interface	4.03	4.55	5.89	5.56
I would use this interface	4.16	4.55	5.83	5.46

Table 3: Stanine scores computed for each statement submitted to the participants for the evaluation of the phone, slider, radar, and bar interfaces

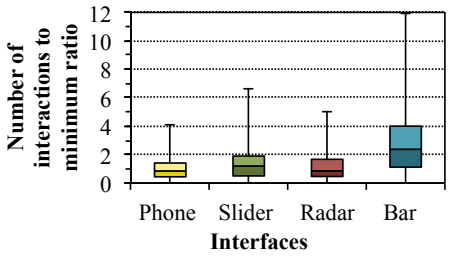


Figure 8: Ratio of the number of interactions compared to the minimal number of expected interactions for the phone, slider, radar and bar interfaces

terface over another by considering their specificities. For the phone and bar interfaces, we asked the participant to rate the following statement using a seven point Likert scale: "*I find the use of green for most safe and red for least safe is easy to understand*". The results show that a large majority of participants agreed with the proposed statement regarding the phone interface (Q_1=4, Q_2=6, Q_3=6) and even stronger, in the case of the bar interface (Q_1=5, Q_2=6, Q_3=7). These results were confirmed by the comments of the participants: 11 participants mentioned that they liked the proposed color mapping for the phone interface, while 19 appreciated it for the bar interface. Several participants further suggested to include the same color mapping to the radar and slider interface. However, other participants highlighted the possible ambiguity in using colors, since red may also be associated to the notion of protection instead of the notion of danger. This ambiguity is though limited in our prototype implementation by a textual hint recalling the degree of granularity associated to each color.

We further analyzed whether the proposed designs cater for an appropriate visualization of the purpose of the interface. We first considered the phone interface and asked if "*the phone background image is a useful indicator of what this interface does*". The ratings of the participants as well as their comments remained neutral regarding this statement, even if a slight agreement can identified (Q_1=4, Q_2=6, Q_3=7). In particular, two participants commented that they did not understand the meaning of the background image. We then compared the scores obtained by the radar and the bar interface regarding the statement: "*I find the bar graph is a useful indicator of how safe the data in my phone is*". Globally, the radar interface obtained better scores (Q_1=5, Q_2=6, Q_3=6) than the bar interface (Q_1=3, Q_2=5, Q_3=6). Several comments confirmed this result for the radar interface, e.g., "*the graph helps to have an over-*

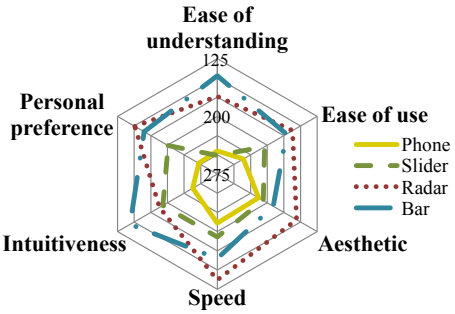


Figure 9: Cumulated scores obtained by the phone, slider, radar, and bar interfaces. A score of 1 indicates the best interface, while a score of 4 indicates the worst interface in the ranking on the participants.

all understanding of the level of privacy", "*the size of the spanned graph gives a good feeling about how safe the settings are*", "*the graph visualization is really smart*".

In conclusion, the radar interface combined with the list interface has been judged by the participants of our user study to the most appropriate interface among the interfaces we proposed according to most evaluation criteria. Based on the comments of the participants, its design can though still be improved. We therefore discuss an enhanced version in the subsequent section.

7. DISCUSSION AND FUTURE WORK

In this paper, we have presented two interfaces allowing users to select people to share pictures with as well as four alternatives to set the associated degree of granularity for the sensor modalities. We have identified preferences of the participants for the list and radar interfaces through the results of our user study. While these results indicate design directions for such interfaces, several aspects can still be improved.

We first plan to take into consideration different comments of the participants of our study regarding the function of the radar interface and integrate them into an enhanced version of this interface. In their final personal comments, several participants complained about the poor usability of the mobile phones, mainly due to the small size and the slow responsiveness of the touchscreen. While these issues are inherent to the nature of the mobile phones, additional efforts could be provided to address these particular aspects. In the case of the radar interface, this implies, e.g., providing bigger radio buttons that are easier for users to interact with as illustrated in Figure 10, which shows an enhanced version of the radar interface. Secondly, participants mentioned that "*the font of the text is too small*" to be easily readable and "*[. . .] not enough information are provided*" about the different options of the interfaces. While increasing the size of the font is relatively easy, providing additional information is more complex. Indeed, adding further information within the same interface may require to reduce the size of the control elements reducing their usability and would overload the interface. Therefore, additional studies should be conducted to further analyze this issue and optimize the provided solution by focusing on the minimum and maximum amount of information to provide and which type of representation is the most appropriate in this case. Thirdly, most of the participants of our study particularly mentioned in their comments that they appreciated the use of colors in the phone and bar interfaces as visual indicator of the current level of privacy protection. Several of them suggested to include the same color mapping in the radar interface. We have therefore

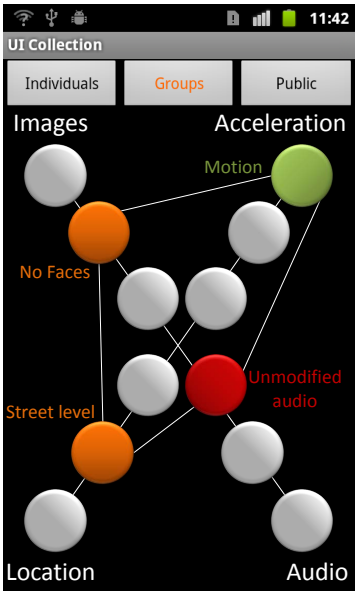


Figure 10: Screenshot of the enhanced radar interface

taken their comments and suggestions into consideration and extended the radar interface with the same color mapping as shown in Figure 10.

In a next step, we envision to refine the design of the enhanced radar interface in order to improve its aesthetics. In fact, the primary objective of this study was to examine how information should be organized and represented to be easily understandable and updated with the fewest interactions as possible. While the aesthetics of the interfaces have been considered during their design, they have nevertheless only taken a secondary role. Finally, we plan to conduct a further user study to evaluate and consequently improve the future version of the radar interface. In the long term, we intend to deploy the interface at a larger scale and in real mobile sensing applications in order to test it under real-world conditions. Once deployed in a real mobile sensing application, we expect the contextualized user behavior to be a more representative indicator of the usability of our approach. Further research questions could be investigated, e.g., how the users change their privacy preferences based on their context, at which frequency such changes take place, or if they fully understand the implications of their choices on their privacy. While the presented interfaces can be used to study these aspects, we consider their investigation as future work.

8. CONCLUSIONS

In this paper, we have presented different privacy interface designs specially tailored for mobile sensing applications. The proposed list and spindle interfaces allow users to select the people to which they want to release the sensor readings collected using their mobile phones, whereas the phone, slider, radar and bar interfaces allow them to select the corresponding degree of granularity for each released sensing modality. We have implemented and evaluated these interfaces by means of an empirical user study. The results show a particular preference of the participants for the radar interface paradigm and provide further insights about potential future improvements. In conclusion, the increasing number of mobile sensing applications will pose new security risks, particularly in the domain of privacy. At the same time, privacy-preserving solutions

are becoming increasingly complex with regards to their configuration process. The outcomes of our study thus pave the way to future applications, in which privacy will be an inherent component.

9. ACKNOWLEDGMENTS

The authors would like to thank the participants of the user study and Alvina Grace Lee for their contributions. This work was supported by CASED (www.cased.de).

10. REFERENCES

[1] The ObscuraCam Application. Online: https://play.google.com (accessed in 06.2012).

[2] The PrivacyCamera Application. Online: https://play.google.com (accessed in 06.2012).

[3] A. Adams and M. Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] A. Brush, J. Krumm, and J. Scott. Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (Ubicomp)*, pages 95–104, 2010.

[5] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick. A Survey on Privacy in Mobile Participatory Sensing Applications. *Journal of Systems and Software*, 84(11):1928–1946, 2011.

[6] L. F. Cranor, P. Guduru, and M. Arjula. User Interfaces for Privacy Agents. *ACM Transactions on Computer-Human Interacteration (TOCHI)*, 13:135–178, 2006.

[7] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma. PRISM: Platform for Remote Sensing using Smartphones. In *Proceedings of the 8th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 63–76, 2010.

[8] N. S. Good and A. Krekelberg. Usability and Privacy: A Study of Kazaa P2P File-sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 137–144, 2003.

[9] N. Győrbíró, Á. Fábián, and G. Hományi. An Activity Recognition System for Mobile Phones. *Mobile Networks and Applications*, 14(1):82–91, 2009.

[10] L. Jedrzejczyk, B. A. Price, A. Bandara, and B. Nuseibeh. "Privacy-shake": A Haptic Interface for Managing Privacy Settings in Mobile Location Sharing Applications. In *Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI)*, pages 411–412, 2010.

[11] A. K. Karlson, A. B. Brush, and S. Schechter. Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 1647–1650, 2009.

[12] P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith, and J. Hightower. Exploring Privacy Concerns about Personal Sensing. *Pervasive Computing*, pages 176–183, 2009.

[13] H. Lipford, A. Besmer, and J. Watson. Understanding Privacy Settings in Facebook with an Audience View. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC)*, pages 1–8, 2008.

[14] H. Lu, W. Pan, N. Lane, T. Choudhury, and A. Campbell. SoundSense: Scalable Sound Sensing for People-centric Applications on Mobile Phones. In *Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 165–178, 2009.

[15] P. Mohan, V. Padmanabhan, and R. Ramjee. Nericell: Rich Monitoring of Road and Traffic Conditions using Mobile Smartphones. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, pages 323–336, 2008.

[16] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang. ACCessory: Password Inference Using Accelerometers on Smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile)*, pages 9:1–9:6, 2012.

[17] R. Rana, C. Chou, S. Kanhere, N. Bulusu, and W. Hu. Ear-Phone: An End-to-end Participatory Urban Noise Mapping System. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 105–116, 2010.

[18] B. N. Schilit, A. LaMarca, G. Borriello, W. G. Griswold, D. McDonald, E. Lazowska, A. Balachandran, J. Hong, and V. Iverson. Challenge: Ubiquitous Location-aware Computing and the "Place Lab" Initiative. In *Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)*, pages 29–35, 2003.

[19] E. von Zezschwitz and A. Hang. Towards Privacy-Aware Mobile Device Sharing. In *4th International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)*, 2012.

[20] A. Whitten and J. Tygar. Why Johnny can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium (SSYM)*, pages 14–29, 1999.