Raising User Awareness about Privacy Threats in Participatory Sensing Applications through Graphical Warnings

Delphine Christin
Secure Mobile Networking Lab
TU Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany

Martin Michalak
Secure Mobile Networking Lab
TU Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt
Mornewegstr. 32
64293 Darmstadt, Germany

firstname.lastname@cased.de

ABSTRACT

Mobile phones are increasingly leveraged as sensor platforms to collect information about user's context. The collected sensor readings can however reveal personal and sensitive information about the users and hence put their privacy at stake. In prior work, we have proposed different user interfaces allowing users to select the degree of granularity at which the sensor readings are shared in order to protect their privacy. In this paper, we aim at further increasing user awareness about potential privacy risks and investigate the introduction of picture-based warnings based on their current privacy settings. Depending on their privacy conception and the proposed warnings, users can then adapt their settings or leave them unchanged. We evaluate the picture-based warnings by conducting a user study involving 30 participants. The results show that more than 70% of the participants would change their settings after having seen the picture-based warnings.

Categories and Subject Descriptors

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, Mobile Computing, Participatory Sensing

1. INTRODUCTION

With over 6 billion subscriptions worldwide [23], mobile phones are ubiquitous and their technological advances have lead to the emergence of millions of novel applications available in, e.g., the Google Play Store [20] or Apple's App Store [4]. The class of participatory sensing apps focuses on the collection of data about the users and their environment using sensors available in their mobile phones, such as accelerometers, cameras, and microphones. Example applications include monitoring diets [33], road and traffic conditions [30], and noise pollution [6]. While these applications could improve the life quality of millions of users, they simultaneously convert mobile phones into "miniature spies" and endanger the privacy of contributing users [14]. For example, pictures can reveal social relationships and visited locations, while accelerometer data can be exploited to identify users' current activities. The spatiotemporal annotations of the sensor readings may further reveal users' routines and habits [34]. Revealing these information to inappropriate parties may have severe consequences for contributing users, such as stalking or burglary.

In order to give users increased control over their privacy, we have investigated different graphical privacy interfaces specially tailored to participatory sensing applications in [13]. By using such interfaces, users can apply filters, which eliminate privacy-sensitive elements of the sensor readings prior to transmission to the application server. The results of our user study show a user preference towards differently colored and sized elements to visualize the current level of privacy protection. Based on these results, we aim at investigating if further information on the consequences of their choice can aid users in finding appropriate privacy settings. To this end, we make the following contributions:

1. We propose to display picture-based warnings matched to the selected sensing modality and degree of granularity. These warnings should allow users to identify potential threats to their privacy and invite them to reflect on their current settings (and maybe modify them accordingly). For each sensing modality and level of privacy protection, different warning scenarios are portrayed in order to prevent users from getting used to them. While we address the application of such warnings in participatory sensing scenarios in this paper, the proposed concept can also be applied in further applications, such as online social networks.

2. We also introduce a history view to allow users to consult who has accessed their data when and at which

MoMM2013, 2-4 December, 2013, Vienna, Austria.

degree of granularity. By analyzing these entries, users can verify whether their current privacy settings correspond to their privacy conception and adapt them if necessary.

3. We integrate our solutions into a prototypical participatory sensing application and evaluate them by means of a user study involving 30 participants. The results are encouraging, as more than 70% of the participants would appreciate having picture-based warnings in participatory sensing applications.

Our paper is structured as follows. In Section 2, we discuss privacy threats related to participatory sensing applications. We introduce the privacy interface serving as basis of this work in Section 3. In Section 4, we describe our solutions, while we detail their evaluation in Section 5 and comment on the results in Section 6. We survey related work in Section 7, before concluding this paper in Section 8.

2. PRIVACY THREATS

In participatory sensing applications, participants gather sensor readings using their mobile phones. Sensor readings include sound samples, pictures, and acceleration data. As shown in [14], almost all applications annotate the collected sensor readings with spatiotemporal information. The annotated sensor readings are then reported to an application server as illustrated in Fig. 1, which is run by the application administrators. Eventually, either the administrators or third parties (e.g., doctors or scientists working in this field) analyze the sensor readings. The analyzed sensor readings are finally released in forms of maps or statistics to the end users including the participants themselves, their relatives, friends, or a larger public. In what follows, we outline potential privacy threats associated to the collection of location information as well as selected sensing modalities.

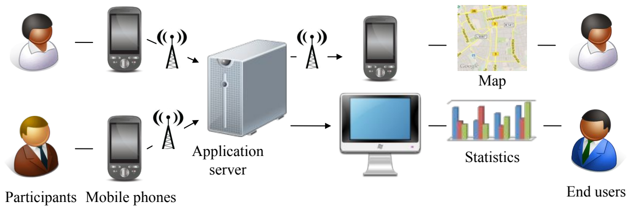


Figure 1: Participatory sensing architecture

2.1 Location

Administrators and potential analysts can have access to locations visited by the users when collecting sensor readings. By using this information, they can infer a wealth of sensitive information about the users. For example, they can determine their habits and routines, infer their identity based on their domicile locations [25], their medical state based on frequent visits to hospitals as well as their political affiliations [34]. Stalkers and robbers can also use this information to harm their victims.

2.2 Pictures

By providing pictures to participatory sensing applications, users can endanger both their and others' privacy. Pictures can provide insights about user behaviors and personalities, their personal environment, and their locations. By using face recognition software and pictures already available online, user identity can even be inferred as shown in [32]. Picture releases may lead to similar consequences as witnessed in online social networks. For example, a woman on sick leave lost benefits from her health insurance after publishing her holidays pictures online [10], while another lost her job as a teacher due to pictures showing her with wine glasses [11].

2.3 Audio Samples

Depending on the granularity at which the audio samples are shared, different information about the users can be revealed. Not only confidential and intimate conversations can be recorded, but current user locations or numbers dialed on their mobile phones can also be inferred. As shown in [31], an analysis of collected sound samples can reveal whether users are in the street, in restaurants, offices, homes, or cars. As a result, similar privacy threats as discussed in Section 2.1 also apply in the case of collected sound samples.

2.4 Acceleration Data

The collection of accelerometer data may appear innocuous to most users. However, their analysis can reveal sensitive information about the users. Their current activities can be recognized among walking, sitting, standing, jogging, biking and driving [26]. Mobile phones worn on user hips may allow to identify gait characteristics and thus provide indications about user identities [17]. Moreover, inputs on phone keyboards, such as text sequences of 6-character passwords, can be extracted from acceleration data as shown in [9] and [22].

2.5 Summary

In summary, each presented sensing modality can compromise user privacy and may have severe consequences, ranging from social to safety and security threats [34]. Most participatory sensing applications collect several of these sensing modalities, thus increasing the risks to user privacy in absence of privacy-preserving mechanisms. Based on this threat analysis, it therefore appears necessary to make users of such applications aware of potential risks to their privacy.

3. PRIVACY INTERFACE

In the remainder of this paper, we assume that users collecting sensor readings can control the release of their data in two dimensions as proposed in [13]. Firstly, they can decide to share their collected sensor readings with particular individuals, groups of individuals, or to make them available publicly. Secondly, they can choose the degree of granularity at which each collected sensing modality is shared. Table 1 illustrates the chosen degrees of granularity associated to each selected sensing modality. The first row corresponds to the finest granularity, i.e., unprocessed raw data, while the third row corresponds to the coarsest degree of granularity. We assume that filters running on the user's mobile phone process the original sensor readings to realize the medium and coarse degrees of granularity. For example, a filter eliminates the frequencies corresponding to human voice from the original sound sample, while another computes its loudness level [29]. 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)

Table 1: Selected degrees of granularity for the different sensing modalities [13]

Granularity degree	Location	Sound	Picture	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)

and whether he is moving based on original accelerometer data [21].

In order to provide users control over the recipients and the degrees of granularity at which data are being shared, we have designed different graphical interfaces in [13] and explored user preferences by means of a user study. Fig. 2 illustrates one of the two interfaces preferred by the 80 users of our prior study. The interface is arranged along two diagonal lines. Each half diagonal is dedicated to a sensing modality and presents three radio buttons, one for each degree of granularity. Touching a radio button changes its color (green for coarse granularity to red for fine granularity) and selects it as current setting. The name of the corresponding degree of granularity also appears. 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. In our prototype implementation, the larger the quadrilateral, the better the privacy protection.

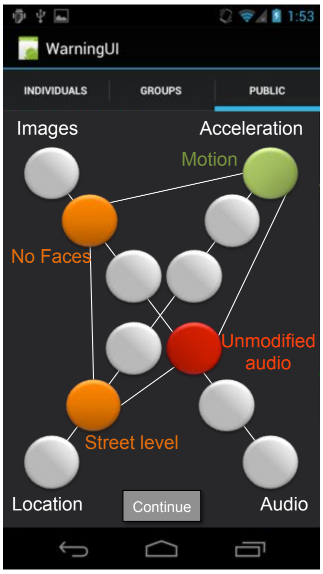
While the presented interface aims at increasing user awareness using both color code and quadrilateral area, we believe that the potential risks discussed in Section 2 should also be illustrated in order to further inform the users. Within the scope of this paper, we therefore build upon this interface and investigate means to reach this goal.

4. INCREASING PRIVACY AWARENESS

Studies in orthogonal domains (e.g., online social networks [28]) have demonstrated that users have difficulties to understand and manage their privacy settings. As a result, most users leave the default settings unchanged and only change them when they have detected privacy intrusions [35]. To avoid these pitfalls in participatory sensing scenarios, we first analyze the design space to support user awareness about potential privacy threats and outline our design drivers in Section 4.1, before presenting our solutions in Sections 4.2 and 4.3, respectively.

4.1 Design Space and Drivers

One solution to inform users about potential consequences of releasing sensitive and personal data could be to add an information button in the proposed interface. By selecting it, users could access an explanative text. Since it would require a dedicated user interaction, not all users may select it. To overcome this issue, a textual warning could automatically pop up after users have selected their settings. However, most users are overwhelmed with such warnings in their daily life, e.g. when they install new software. Only few users may take the time to read the warnings in detail, while the rest may just ignore them. Both options are therefore not considered as appropriate to efficiently increase user awareness. In order to inform users about potential risks, we believe that any solution should:



Images
Acceleration
Motion
No Faces
Unmodified audio
Street level
Location
Audio

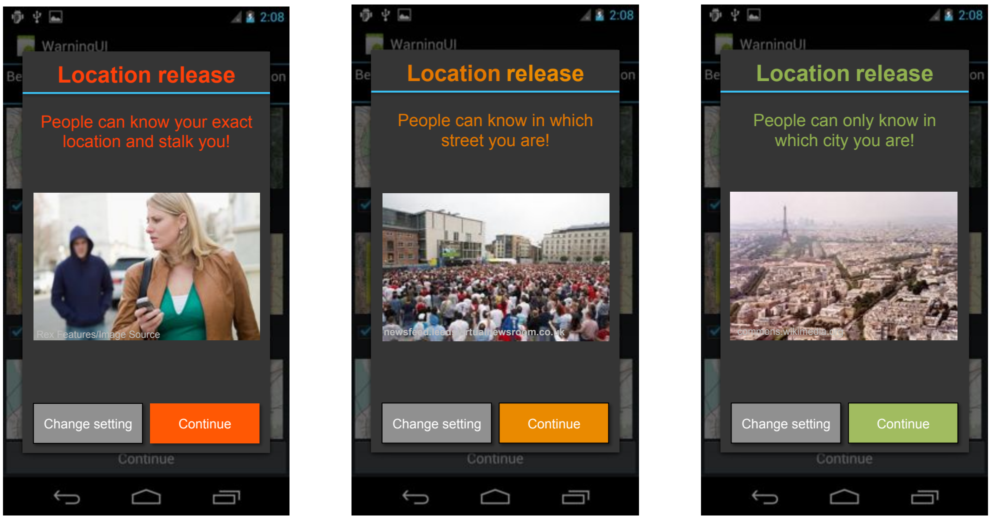
Figure 2: Example of privacy settings selected in the underlying privacy interface

- not require a specific user interaction
- not be time-consuming
- be comprehensible
- be easy to use
- be tightly coupled with the current settings in the underlying privacy interface
- illustrate the consequences of users' choices, and
- be adapted to the limited size of phone displays

In the following sections, we present our designs based on the above design drivers. Note that we investigate whether our solutions reflect these drivers using a user study detailed in Section 5.

4.2 Picture-based Warnings

Based on the above design drivers, we propose to use dynamic picture-based warnings to increase user awareness. Inspired by pictures on cigarette packets illustrating risks of smoking, our solution aims at addressing users directly. Instead of using complex textual description, our objective is to illustrate the threats in form of pictures easily comprehensible by the users. For each sensing modality and associated degrees of granularity, we propose different scenarios illustrating potential associated risks. We further randomize their occurrences in order to maintain user attention. Each warning includes a picture and a sentence about the illustrated threat. If the warnings appeal to users, they can directly access the underlying interface (see Section 3) by a dedicated button located in the pop up window. We reuse the color code of our prior interface for the description and the "continue" button—green for a coarse-granular setting, orange for a moderate one, and red for a fine-granular one.



Location release

People can know your exact location and stalk you!

Location release

People can know in which street you are!

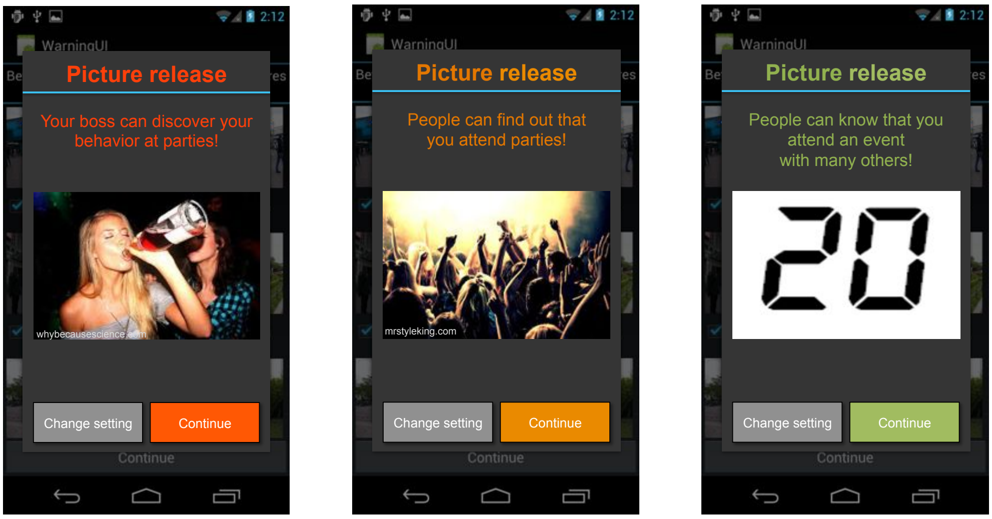
Location release

People can only know in which city you are!

2:08
WarningUI
Rex Features/Image Source
newsfeed.ieee/virtualnewsroom.co.uk
commons.wikimedia.org
Change setting
Continue

(a) Fine-granular setting (b) Medium setting (c) Coarse-granular setting

Figure 3: Example of warning messages when users release location data at different degrees of granularity



Picture release

Your boss can discover your behavior at parties!

Picture release

People can find out that you attend parties!

Picture release

People can know that you attend an event with many others!

(a) Fine-granular setting (b) Medium setting (c) Coarse-granular setting

Figure 4: Example of warning messages when users release pictures at different degrees of granularity

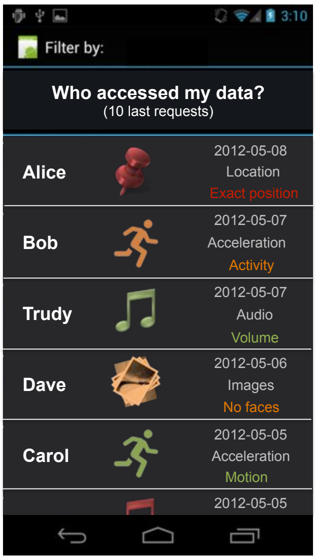
Due to the presence of the explanatory sentence, our design does not only rely on a color code and is thus also usable by colorblind people. When having completed the selection, users can access the data to be shared. These data are displayed at the same resolution as selected by the users in their settings. Users can hence determine which data they want to share based on a visualization of the possible consequences and the knowledge of the outcome of the applied filter.

4.2.1 Examples

In this section, we present two examples of warning sets we designed. The former set addresses threats to location privacy, while the latter illustrates potential risks when publishing pictures online. Note that the design possibilities are not limited to these sensing modalities and chosen scenarios.

As shown in Fig. 3, we first illustrate the risks of being stalked when sharing location information. If users decide to share their precise position using the underlying interface presented in Fig. 2, the warning represented in Fig. 3(a) will be displayed. When choosing to share the street or city names, users will see the warnings illustrated in Fig. 3(b) and 3(c), respectively. The scenarios can be freely configured and include scenarios involving, e.g., visits to political events, hospitals, or strip clubs, as well as risks of robbery and theft.

Fig. 4 shows our warning set on the risks of sharing party pictures depending on the selected degree of granularity. In particular, Fig. 4(a) illustrates impressions that an employer may get about employees, when those select to share pictures at this granularity. In comparison, it is more difficult to infer the identity of the person when applying the moderate setting as shown in Fig. 4(b). From the number of present



3:10

Filter by:

Who accessed my data?
(10 last requests)

Alice — 2012-05-08 — Location — Exact position

Bob — 2012-05-07 — Acceleration — Activity

Trudy — 2012-05-07 — Audio — Volume

Dave — 2012-05-06 — Images — No faces

Carol — 2012-05-05 — Acceleration — Motion

2012-05-05

Figure 5: Screenshot of the history interface

people on pictures, only little information about the users is revealed, e.g., whether the users are solitary or sociable. In addition to the topic of alcohol and party, warning messages could be composed in the setting of personal hobbies or home interiors.

4.3 History View

In addition to the picture-based warnings, we propose a history view shown in Fig. 5, in which users can obtain statistics about the accessed data. By offering this view, we aim at outlining how real the sharing is and thus increasing user awareness even further. Users can consult who had access to which data at which degree of granularity and when. Again, the same colors are used to code the different degrees of granularity and allow fast user recognition of potential threats to privacy. Additionally, users can verify whether their privacy settings match their privacy conception. In case of mismatch, they can directly access the underlying privacy setting interface to modify them. To help the users, the history can be filtered according to different criteria, such as sensor modality, data recipients, or access dates. Summaries about, e.g., the most accessed sensing modalities in the last day or weeks, are also available.

In summary, we propose to use both picture-based warnings and a history view to increase the transparency of the sharing process as well as the associated threats for the users. In particular, we present users with data at the same resolution they are shared, thus making the filtering process tangible.

5. USER STUDY

We have integrated our solutions into a prototypical participatory sensing application and performed an empirical user study to evaluate them. We have recruited our participants by posting announcement on different forums and mailing lists in different departments of our university. In total, 30 participants volunteered to contribute to our evaluation and experience both the picture-based warnings and the proposed history view. The participants were rewarded for their contribution with refreshments, no monetary remunerations were offered. The study took approximately one hour per participant in average. In this section, we first detail our study settings in Section 5.1 and present the demographics of our participants in Section 5.2, before commenting on the corresponding results. Sections 5.3 and 5.4 address the evaluation of the picture-based warnings and the history view respectively, while Section 5.5 focuses on the usability and user acceptance and Section 5.6 on user comments.

Table 2: Privacy settings to be configured by the participants in the first two study tasks

Task	Granularity degree	Location	Sound	Picture	Acceleration
1	Fine	x			x
	Medium			x	
	Coarse		x		
2	Fine			x	
	Medium	x	x		
	Coarse				x

5.1 Study Settings

We distributed a paper leaflet including instructions and questions to the participants of our study as well as a Google Galaxy Nexus phone with our prototype to test our solutions. After an introduction to participatory sensing applications and a brief description of the privacy setting interface illustrated in Fig. 2, we provided instructions to conduct three different tasks. In the first task, participants needed to configure their privacy settings to share data with an individual according to the given degrees of granularity shown in the first line of Tab. 2. After having experienced the location warning, the participants were asked to change the corresponding setting to a coarser granularity and observe potential changes in the representation of the data to be published. In the second task, the participants configured the settings to share data with the public according to the second line of Tab. 2. At this stage, we asked the participants to observe the location information to be published and compare them to those of the first task. Additionally, the participants could change the settings of other sensing modalities as they desired in order to experience the corresponding warning(s). Finally, we asked the participants to consult the history view and filter predetermined results according to a given timespan. After fulfilling these three tasks, the participants were asked to answer a set of questions about their demographics and experience with the tested solutions.

5.2 Demographics

Among the 30 participants of our user study, 90% were male and 10% female. Their age ranged between 19 and 49 years with an average of 25. A majority (87%) were undergraduate students, while the remaining were employees at our university. The education fields were distributed among computer science (33%), business economics (20%), chemistry (10%), mathematics (5%), and others. While our sample is not representative for the whole population, it specially focuses on potential users of participatory sensing applications [12] with existing online sharing experience. In our sample, 80% of the participants have already published data online (80% of which still do it at least once a month) and 10% are active users of participatory sensing applications.

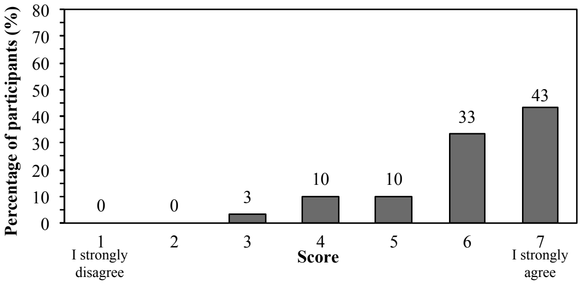


Figure 6: Answer distribution to the statement: "It is easy to understand the differences between the selectable privacy levels"

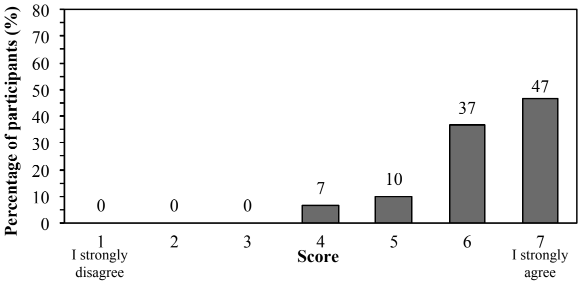


Figure 7: Answer distribution to the statement: "It is easy to understand which data are published"

5.3 Privacy Settings and Warnings

We present the answers given by the participants about the privacy interface and the picture-based warnings. Our questions focus on the comprehensibility and transparency of the publishing process perceived by potential users. To evaluate these aspects, we first submitted the following statement to the user "It is easy to understand the differences between the selectable privacy levels" and asked them to indicate their degree of agreement with this statement using a 7-point Likert scale. The distribution of the participants' answers is displayed in Fig. 6 and show that more than 85% of participants agreed with this statement (the *first quartile* $Q_1 = 6$, the *second quartile* $Q_2 = 6$, and the *third quartile* $Q_3 = 7$). Moreover, more than 85% of participants found that "it is easy to understand which data are published" as detailed in Fig. 7 ($Q_1 = 5, Q_2 = 6, Q_3 = 7$).

About the picture-based warnings, all participants except one found that "the warnings are easy to understand" (see Fig. 8) ($Q_1 = 6, Q_2 = 7, Q_3 = 7$). Moreover, all participants agree with the statement "The warnings help me to understand which threats are possible when using such an application" by choosing a score higher than four ($Q_1 = 6, Q_2 = 6, Q_3 = 7$). In order to investigate the impact of the warnings, we asked if the participants "[felt] addressed by the chosen warning scenarios". As shown in the Fig. 9, 70% of participants agreed with this statement ($Q_1 = 4, Q_2 = 5, Q_3 = 6$). One participant who did not feel addressed commented that "[he knew] the individuals with whom [he shares his] data, thus the [stalking] scenario does not apply in this case". Another participant indicated that "for [him] the warnings are addressed to users with only little knowledge about data privacy and its consequences". Since the participants were more divided about this statement than for the previous ones, we discuss the difficulty to find appropriate scenarios and pictures in Section 6. Additionally, we were interested in knowing whether participants would change their privacy settings after having seen the warnings. Fig. 10 illustrates the results and shows that 73% would modify them, 17% would not, and 10% are undecided ($Q_1 = 4, Q_2 = 5, Q_3 = 6$). While these results do not reflect the participants' behavior under real-world conditions, they however outline that the chosen graphical representations are very likely to impact the privacy decisions of the participants. We went a step further by asking if "the warnings would impact [their] decision to contribute to participatory sensing applications". Fig. 11 shows that 50% of the participants would opt out, whereas 30% would continue to contribute and the remaining was undecided ($Q_1 = 3, Q_2 = 4.50, Q_3 = 6$). Again, this demonstrates the efficiency of the warnings based on the participants' claims. On the other side, informing users about the privacy threats of such applications may endanger the viability of participatory applications. Consequently, application administrators may not be willing to embed such warnings to maintain their user bases, thus limiting the deployment of our solution at large scale.

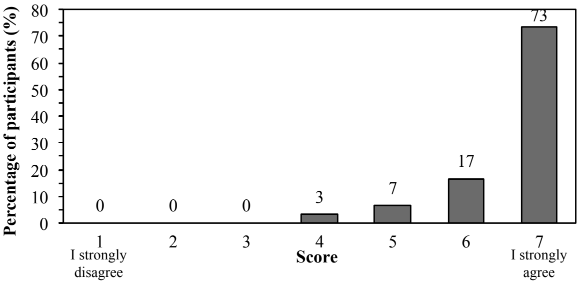


Figure 8: Answer distribution to the statement: "The warnings are easy to understand"

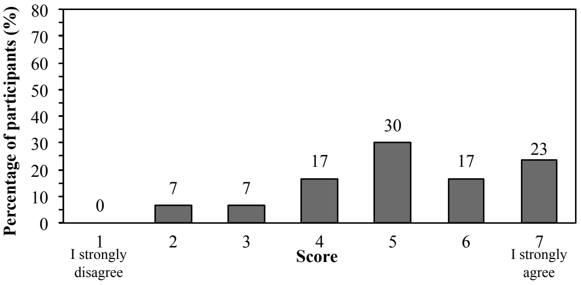


Figure 9: Answer distribution to the statement: "I feel addressed by the chosen warning scenarios"

In summary, participants understood both warning content and necessity. Most participants found the scenarios adequate and felt addressed by them. As detailed in Section 6, we however believe that personalized scenarios can further increase the warning impacts by adapting them to, e.g., the user gender. In their current version, the warnings already influence a large majority of participants who claim that they would change their privacy settings or even opt out after having seen the warnings. While increasing user awareness about privacy threats can put the viability of participatory sensing applications at risk, we believe that

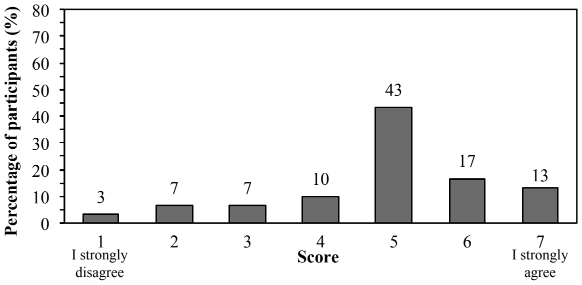


Figure 10: Answer distribution to the statement: "I would modify my privacy settings after having seen the warnings"

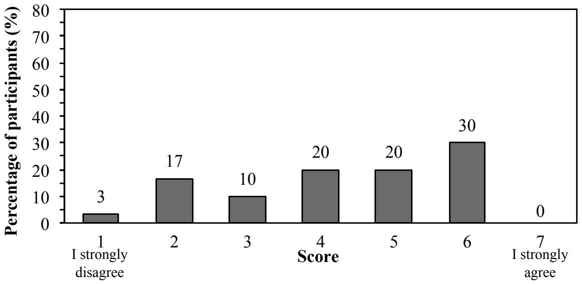


Figure 11: Answer distribution to the statement: "The warnings would impact my decision to contribute to participatory sensing applications"

users should take conscious decisions and balance the risks for their privacy compared to the benefits provided by the applications.

5.4 History View

In the third task of our study, participants tested the history view in order to control who accesses which data when. As illustrated in Fig. 12 and Fig. 13, all participants indicated that "[they] understand the presented information in the history view" ($Q_1 = 6, Q_2 = 6.50, Q_3 = 7$) and more than 80% of the participants are interested in knowing who accessed their data ($Q_1 = 6, Q_2 = 6, Q_3 = 7$). However, around 30% of all participants found that the provided information is insufficient. In their comments, they express the wish to know the purpose of the data access and the context of this access. For example, they would like to know whether the access is for personal or commercial ones or initiated by public authorities. Several participants expressed concerns about the exploitation of their data for marketing purposes or in legal actions. While we can easily integrate this information in our history view, it may be difficult to verify the reliability of the purposes indicated by potential data consumers. Additionally, some participants would appreciate to know the requester locations and wish a finer granularity for the access data. Instead of only knowing the access dates as in our current prototype, they would like to be able to consult the exact access time. Finally, we asked under which conditions participants would modify their privacy settings based on the information present in the history view. Around 80% of the participants indicated that they would change their settings if they notice that strangers have accessed their data, 70% in case of a particular user, and 40% if a sensing modality is frequently accessed.

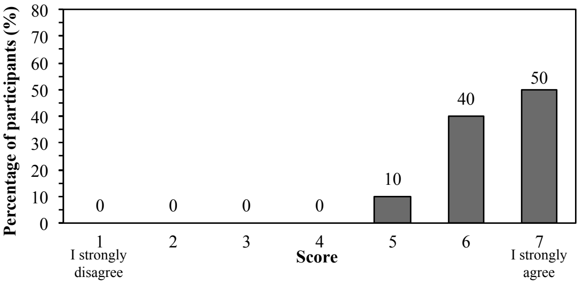


Figure 12: Answer distribution to the statement: "I understand the presented information in the history view"

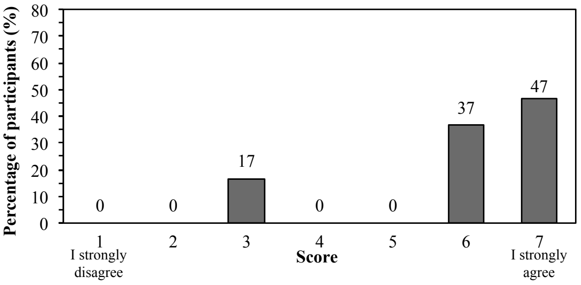


Figure 13: Answer distribution to the statement: "I am interested in knowing who accessed my data"

In summary, all participants understood which information is displayed in the history view and most of them are interested in the displayed content. Some of them even wish finer information granularity. Additionally, participants are more interested in knowing the requester identities and purposes than the nature of the accessed data.

5.5 Usability and User Acceptance

At last, we considered the privacy configuration process as a whole and asked the participants to judge its usability. Among our participants, 70% "[found] the data publishing process easy", whereas around 13% disagreed and the rest remained undecided as seen in Fig. 14 ($Q_1 = 4, Q_2 = 6, Q_3 = 6.50$). Several participants commented that too many interactions are necessary until the data are finally published. While the number of interactions can still be optimized, we believe that it is part of the price to pay to increase ones' awareness and control over their privacy protection. Almost the same distribution can be observed about the assessment of the process duration (cf. Fig. 15). Around 70% "[found] that configuring the settings is fast", 17% disagreed and 13% remained neutral ($Q_1 = 4, Q_2 = 6, Q_3 = 6$). One participant especially indicated that the overhead is too large when publishing sparse data, while it may be appropriate for large data volumes. Another participants added that he "had to de-select the publish check boxes manually". Depending on the user-sharing pattern, it may be faster to select or deselect the data to be published or not. Therefore, no universal solution can be found to save configuration time. Despite the fact that most participants assess the process as fast, we believe that this impression can be improved in a real-world

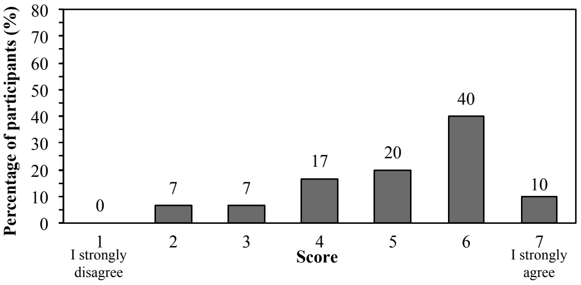


Figure 14: Answer distribution to the statement: "I find the data publishing process easy"

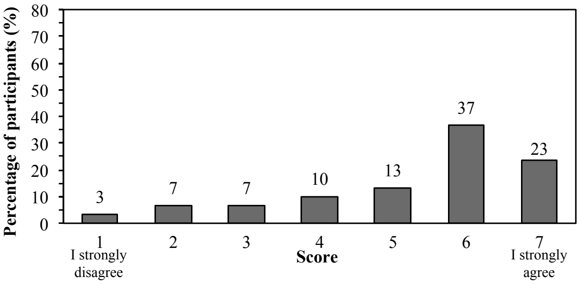


Figure 15: Answer distribution to the statement: "I find that configuring the settings is fast"

setting as we forced the participants to go through the whole publishing process twice for evaluation purpose within the scope of our study.

We finally asked whether the participants "would like to have such warnings in other applications". A large majority (more than 70%) would appreciate it as compared to 10% who would not, the rest remaining undecided as shown in Fig. 16 ($Q_1 = 4, Q_2 = 6, Q_3 = 7$). Similarly, over 75% of the participants "would like to have an history view in other applications" (Fig. 17). In comparison, 10% were not interested in such information, while the remaining was neutral ($Q_1 = 5, Q_2 = 6, Q_3 = 7$).

In summary, the majority of our participants found that configuring their sharing settings is fast and easy. Moreover, they would like to have similar warnings and history view in further applications.

5.6 User Comments

At the end of our questionnaire, we gave the opportunity to the participants to comment and/or make suggestions on our proposed solutions. One participant suggested to also including settings for the warnings, so users could determine how many warnings are displayed. Another participant wished to have a process bar indicating the remaining number of steps to perform. Indeed, some participants needed some time to figure out that they should click on the "continue" button to pursue the process. A further participant stated that "[he liked] the usage of different colors for the different privacy levels".

As a result, most answers provided by the participants confirm the realization of our design drivers in our proof-of-concept implementation and show their enthusiasm for the proposed solutions. In addition to their answers, their spontaneous reactions show that they understood the necessity to display warnings, which data are published, and which settings guarantee the best privacy protection. Based on their feedback, we plan to further improve our prototype by adding a progress bar to show how many steps still need to be conducted, for example.

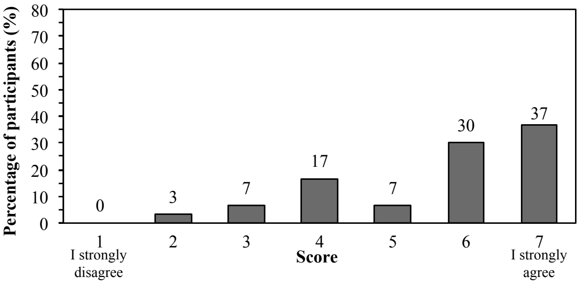


Figure 16: Answer distribution to the statement: "I would like to have such warnings in other applications"

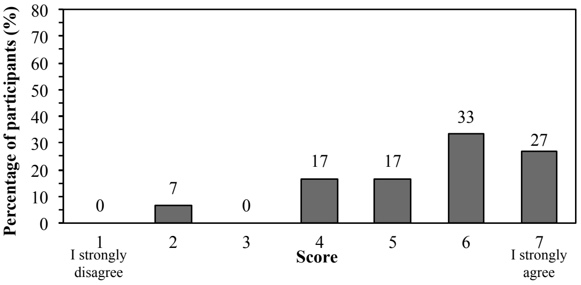


Figure 17: Answer distribution to the statement: "I would like to have a history view in other applications"

6. DISCUSSIONS

As mentioned by one participant, we could fine-tune the warning appearance based on user preferences, such as sensing modality or frequency. While this may optimize their effects, it would also require the users to again personalize settings according to their preferences. By increasing the user overhead, it may become cumbersome for the users. However, we could further investigate whether the warning associated to a coarse-granular setting need necessarily to be displayed, as less privacy threats exist. On the other side, information about the users is still reported to the applications.

Additionally, we could envision to tailor the scenarios illustrated in the picture-based warnings to user profiles. Indeed, finding scenarios adapted to the whole user base may be challenging, as many factors, such as gender or age, can influence to which extent users feel addressed by the warnings. In addition to the scenarios themselves, the choice of the associated pictures is demanding, as our design requires three different privacy levels for each sensing modality and some sensing modalities are more difficult to illustrate than others. When designing the warnings proposed in our study, we therefore encountered difficulties to find both scenarios and pictures able to catch users' attention while not exaggerating about potential risks and simultaneously addressing the widest range of users. To find appropriate scenarios, a subtle balance between provocation, decency, and efficiency needs to be found. We thus believe that additional knowledge, such as cultural background or gender, could improve the impact of the warnings, while respecting user privacy.

7. RELATED WORK

Related work can be classified according to three categories: (1) privacy concerns, (2) privacy interfaces, and (3) privacy warnings. Several user studies have been conducted to analyze user privacy concerns when sharing different sensing modalities with diverse audiences in participatory sensing applications. Privacy concerns while sharing pictures are analyzed in [3], whereas location sharing is investigated in [8, 15]. Similarly to our results, the latter study demonstrates that the user willingness to share location information highly depends on the identity of the data recipient. Additional sensing modalities are examined in [24]. The results indicate that participants are more concerned when sharing location and audio data than accelerometer and barometric data.

Moreover, different user privacy interfaces have been designed and investigated in different 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 [16], [19], and [28, 35], respectively. In [27], common design flaws of privacy interfaces have been identified and guidelines have been provided. Concerning participatory sensing applications, we have proposed and investigated six different interfaces allowing users to select their privacy preferences [13]. As detailed in Section 3, we developed interfaces for selecting users as well as the granularity at which the data are published.

More specifically studies on warnings were conducted in [5, 7, 18, 36]. In [5], the authors introduced colored hints to indicate how many friends have authorized third applications to access different data types. When few friends authorize a data type, the associated field is marked in red, while it is green on the contrary. The authors then analyze the impact of these social hints on the user decisions to authorize access to their own data. In comparison, Bravo-Lillo et al. examined in [7] the differences between novice and advanced users in terms of warning perception and responses based on their mental models. [18] focuses on the efficiency and consequences of warnings in the case of phishing attacks, while [36] concentrates on SSL certificate warnings.

To the best of our knowledge, we are therefore the first to have introduced picture-based warnings to increase the user awareness about potential threats to privacy in participatory sensing applications and evaluate them using a user study.

8. CONCLUSIONS

In this paper, we have investigated new methods to increase user awareness about potential privacy threats associated to sensor data contributions to participatory sensing applications. Based on our existing privacy interface, we have introduced picture-based warnings and a history view in order to reach this objective. By using our solutions, users can be informed about potential risks when submitting data to participatory sensing applications without the need to read lengthy texts. They can also consult who accessed their data at which time and granularity and hence verify whether these accesses are aligned with their privacy conception. As a result, the proposed solutions aspire to make the sharing process transparent and tangible for potential users. In order to evaluate our solutions, we integrated them into a proof-of-concept implementation and conducted a user study with 30 participants. The results show that most participants found the picture-based warnings easy to understand and would be influenced by them when choosing their privacy settings. Additionally, they would like to have such warnings and access view in other applications. Based on these encouraging results, we therefore plan to study their applicability in other domains and compare them to text-based warning methods. We further will conduct long-term user studies to quantify their effects on user behaviors under real-world conditions.

Acknowledgment

This work was supported by CASED (`www.cased.de`) and EC SPRIDE (`www.ec-spride.de`). Our thanks go to A. Reinhardt.

9. 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] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 357–366, 2007.

[4] Apple Inc. Apple Apps on the App Store. Online: `http://www.apple.com/iphone/from-the-app-store/` (accessed in 05.2013), 2013.

[5] A. Besmer, J. Watson, and H. R. Lipford. The Impact of Social Navigation on Privacy Policy Configuration. In *Proceedings of the 6th ACM Symposium on Usable Privacy and Security (SOUPS)*, pages 7:1–7:10. ACM, 2010.

[6] M. Bilandzic, M. Banholzer, D. Peev, V. Georgiev, F. Balagtas-Fernandez, and A. De Luca. Laermometer: A Mobile Noise Mapping Application. In *Proceedings of the 5th ACM Nordic Conference on Human-Computer Interaction (NordiCHI)*, pages 415–418, 2008.

[7] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[8] 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.

[9] L. Cai and H. Chen. TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion. In *Proceedings of the 6th USENIX Conference on Hot Topics in Security (HotSec)*, pages 9–9, 2011.

[10] CBC News. Depressed Woman Loses Benefits over Facebook Photos. Online: `http://www.cbc.ca` (accessed in 05.2013), 2009.

[11] CBS News. Did the Internet Kill Privacy? Facebook Photos Lead to a Teacher Losing her Job; What Expectations of Privacy Exist in the Digital Era? Online: http://www.cbsnews.com (accessed in 05.2013), 2011.

[12] D. Christin, C. Büchner, and N. Leibecke. What's the Value of Your Privacy? Exploring Factors That Influence Privacy-sensitive Contributions to Participatory Sensing Applications. In *Proceedings of the IEEE Workshop on Privacy and Anonymity for the Digital Economy (LCN Workshop)*, 2013.

[13] D. Christin, A. Reinhardt, M. Hollick, and K. Trumpold. Exploring User Preferences for Privacy Interfaces in Mobile Sensing Applications. In *Proceedings of 11th ACM International Conference on Mobile and Ubiquitous Multimedia (MUM)*, pages 14:1–14:10, 2012.

[14] 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.

[15] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 81–90, 2005.

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

[17] M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive User-authentication on Mobile Phones using Biometric Gait. In *Proceeding of the 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 306–311, 2010.

[18] S. Egelman, L. F. Cranor, and J. Hong. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI/ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1065–1074, New York, NY, USA, 2008.

[19] 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.

[20] Google Inc. Google Play Store. Online: https://play.google.com (accessed in 05.2013), 2013.

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

[22] J. Han, E. Owusu, L. Nguyen, A. Perrig, and J. Zhang. ACComplice: Location Inference using Accelerometers on Smartphones. In *4th International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–9, 2012.

[23] International Communication Union. The World in 2013: ICT Facts and Figures. Online: http://www.itu.int (accessed in 05.2013), 2013.

[24] P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith, and J. Hightower. Exploring Privacy Concerns about Personal Sensing. In *Proceedings of the 7th International Conference on Pervasive Computing (Pervasive)*, pages 176–183, 2009.

[25] J. Krumm. Inference Attacks on Location Tracks. In *Proceedings of the 5th IEEE International Conference on Pervasive Computing (Pervasive)*, pages 127–143, 2007.

[26] J. R. Kwapisz, G. M. Weiss, and S. A. Moore. Activity Recognition using Cell Phone Accelerometers. *SIGKDD Explorations Newsletter*, 12:74–82, 2011.

[27] S. Lederer, I. Hong, K. Dey, and A. Landay. Personal Privacy through Understanding and Action: Five Pitfalls for Designers. *Personal Ubiquitous Computing*, 8(6):440–454, 2004.

[28] H. R. Lipford, J. Watson, M. Whitney, K. Froiland, and R. W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In *Proceedings of the 28th International ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1111–1114, 2010.

[29] H. Lu, W. Pan, N. D. Lane, T. Choudhury, and A. T. 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.

[30] 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.

[31] V. Peltonen, J. Tuomi, A. Klapuri, J. Huopaniemi, and T. Sorsa. Computational Auditory Scene Recognition. In *Proceedings of the 27th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, volume 2, pages II–1941–II–1944, 2002.

[32] F. Y. Rashid. Facial-Recognition Tools, Facebook Photos Threaten End to Anonymity: Study. Online: http://www.eweek.com, Aug. 2011.

[33] S. Reddy, A. Parker, J. Hyman, J. A. Burke, D. Estrin, and M. Hansen. Image Browsing, Processing, and Clustering for Participatory Sensing: Lessons from a DietSense Prototype. In *Proceedings of the 4th Workshop on Embedded Networked Sensors (EmNets)*, pages 13–17, 2007.

[34] K. Shilton. Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection. *Communications of the ACM*, 52(11):48–53, 2009.

[35] K. Strater and H. R. Lipford. Strategies and Struggles with Privacy in an Online Social Networking Community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers (BCS-HCI)*, volume 1, pages 111–119, 2008.

[36] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the 18th Conference on USENIX Security Symposium (SSYM)*, pages 399–416, Berkeley, CA, USA, 2009. USENIX Association.