Delphine Christin, Christian Roßkopf, Matthias Hollick: *uSafe: A Privacy-aware and Participative Mobile Application for Citizen Safety in Urban Environments*. In: Pervasive and Mobile Computing, 9(5), pp. 695-707, 2013.

uSafe: A Privacy-aware and Participative Mobile Application for Citizen Safety in Urban Environments

Delphine Christin, Christian Roßkopf, Matthias Hollick

Secure Mobile Networking Lab
Technische Universität Darmstadt
Mornewegstr. 32, 64293 Darmstadt, Germany
Phone +49 6151 16-70922, Fax: +49 6151 16-70921
E-Mails: firstname.lastname@seemoo.tu-darmstadt.de

Abstract

Recent mobile applications empower citizens to monitor noise pollution or report on features of their urban environment. One important aspect of urban life has, however, not been sufficiently addressed, namely the citizens' safety. We present a privacy-aware application called uSafe, in which users indicate how safe they feel in geographical locations. These feelings are then consolidated into summary maps accessible by other users and urban planners. We evaluate our concept with a questionnaire-based study involving 183 participants. The results confirm the utility of uSafe and show that privacy protection is a decisive factor in their decision to contribute to it.

Keywords:
Urban pervasive application, safety, user-centered, privacy

1. Introduction

Recent mobile phones feature an increasing number of sensors (e.g., microphones, cameras, accelerometers, and gyroscopes), multiple wireless technologies (e.g., Wi-Fi, 3G, and Bluetooth), positioning systems (e.g., GPS, Wi-Fi triangulation), as well as advanced processing and storage capabilities. In addition to these technological features, the wide adoption of mobile phones by the public has lead to the rise of a new paradigm known as participatory or urban sensing [1, 2]. The key idea behind urban sensing is to empower citizens to collect and share sensed data from their surroundings.

A wide range of applications based on this paradigm have emerged in recent years. For example, PEIR [3] computes the degree of exposure users experience to environmental pollutants, Laermometer [4] and Ear-Phone [5] monitor noise pollution in urban environments by analyzing sound samples, and Nericell [6] leverages accelerometers, microphones, and positioning systems to detect and localize traffic and road conditions.

Existing applications mainly concentrate on the collection of sensor readings, which provide factual information about the environment. However, they fail to capture subjective feelings experienced by the users in urban environments, such as how safe citizens feel when walking in different parts of the city. Furthermore, no attention has been paid to the issue of safety in the city. This issue, however, concerns a large number of citizens as shown by, e.g., the statistics of the Criminal Police Office of the Federal Republic of Germany. In the year of 2009, more than 6 million crimes were recorded, including around 92,500 cases of pickpocketing, 370,000 cases of slight bodily injury, and 49,000 robberies [7].

We therefore propose the uSafe application, which aims to inform citizens about safety issues in urban environments based on user-generated content and using mobile devices. The uSafe application has been designed with two key aspects in mind: participation and privacy awareness. As a result of its participatory nature, uSafe is based on contributions of citizens who report their feeling of safety through the use of their mobile phones. Since each user has an individual perception of safety, which can be influenced by various factors such as demographics or time of day, only direct participation of the citizens can enable the collection of such subjective feelings. Using uSafe, the citizens are virtually transformed into a new type of sensor, measuring the pulse of the city in terms of safety. The reported feelings of safety are then compiled at an application server in order to build maps that show the prevailing safety feeling prevailing in different sectors of the city. These maps can be consulted by other participants to, e.g., determine the safest route to a destination. Moreover, these maps provide information useful for urban planning, and can be consulted in order to make problematic areas safer, thus providing a valuable tool for public bodies. Since the viability of uSafe depends on the contributions of citizens, their participation is encouraged and fostered by protecting their anonymity and privacy. In fact, users may refuse to contribute if they feel that their anonymity and privacy may be endangered [8]. We have therefore specifically considered both aspects during the design phase of uSafe, which features different privacy- and anonymity-

preserving mechanisms, fully customizable by users according to their privacy preferences. These mechanisms include location cloaking, the definition of privacy areas, and the utilization of periodic pseudonyms generated using blind signatures. While these mechanisms have already been introduced and analyzed from a theoretical perspective, they often remain hidden from the users who may not be aware of their existence and/or do not have any direct access to them [9]. In uSafe, we partially reveal these mechanisms to users in a practical and usable manner in order to actively involve them in their own privacy decisions. Depending on their individual privacy conception, users can freely decide to apply these mechanisms.

Our contributions can be summarized as follows.

1. We present a mobile application capturing a novel dimension of urban life: the subjective perception of safety.
2. We evaluate the concept of the uSafe application by means of an online questionnaire involving 183 participants. The results show that the majority of the participants would be ready to contribute to uSafe and that the protection of their privacy is a decisive factor in their decision.
3. We propose a privacy-aware architecture and present a prototype implementation for the realization of the entire uSafe application.

The remainder of this article is structured as follows. In Section 2, we present the key objectives of uSafe and explain its operation using an example. We highlight the results of our study in Section 3, and we provide details about the uSafe architecture as well as the prototype implementation in Section 4. In Section 5, we discuss different sociological aspects related to the deployment of uSafe and address related work in Section 6, before making concluding remarks in Section 7.

2. Key Features and Application Scenario

In this section, we highlight the key features of the uSafe application and illustrate its principles by describing a potential application scenario. Note that uSafe is not restricted to this particular scenario, but can be applied in a wide range of other settings.

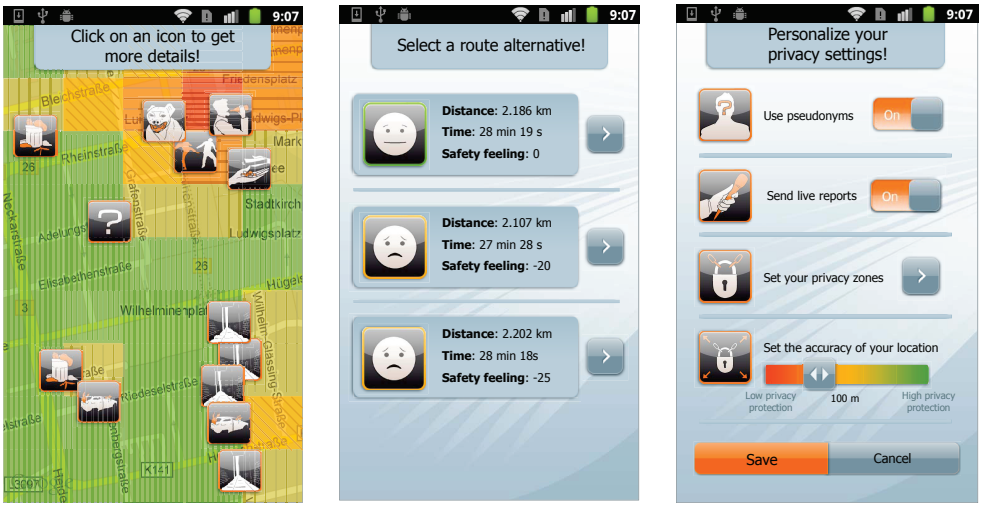
2.1. Key Features

The key features of the uSafe application can be summarized as follows. (1) uSafe is a participative application, which allows users to report their

subjective perception of safety in urban environments. (2) The reported information is made available to all users in the form of maps. The maps allow users to visualize how areas have been rated in terms of safety by other users, and provide details about these ratings, e.g., the reason for such rating. They also support safety-aware route planning and instantaneous notification upon entering unsafe areas. (3) Since the reported information is publicly available, uSafe supports different mechanisms to protect the anonymity and location privacy of the users. These mechanisms can be activated or deactivated by the users according to their privacy preferences. The anonymity protection can be ensured by the utilization of periodic pseudonyms or the definition of privacy zones. In these zones, the reports need to be individually authorized by the users in order not to reveal sensitive locations, which may lead to the identification of the user. Additionally, users can preserve their accurate location by cloaking it, i.e., reporting a bounding box instead of the precise location. They can also delay the reporting process in order to hide their current location. Depending on the granularity and amount of the reported data, rewards for contributing to uSafe are offered to the users.

2.2. Exemplary Application Scenario

We assume that Alice has just moved into a new city. She registers with uSafe to check the city areas, in which safety threats have been reported by other users. Additionally, Alice configures uSafe to inform her when she is about to enter a dangerous area by making her mobile phone vibrate according to a personalized pattern. When Alice is invited for dinner by her new colleague Bob, she looks for the directions between her office and Bob's apartment. Since both locations are within walking distance, Alice decides to walk there and uses uSafe to find a safe route. uSafe proposes three alternative routes to Alice, and provides the following details about each of them: estimated time to destination, distance, and the average reported safety feeling in a range from 0 (very safe) to -100 (very unsafe), as illustrated in Fig. 1(b). Alice decides to follow the first and safest route to Bob's apartment, even if it is not the shortest one. After dinner, Alice walks home and follows the directions given by Bob. At a crossroad, her mobile phone vibrates indicating that she is about to enter a critical zone. Bob, however, had mentioned that some streets may make her feel insecure because of insufficient street lighting, but in his eyes, the area is otherwise known to be safe. Alice thus continues her route and arrives home without any trouble.



(a) Heat map of safety ratings

(b) Path statistics

(c) Privacy settings

Figure 1: Selected screens of the uSafe user interfaces

After a few weeks of usage, Alice decides to contribute to the uSafe application. However, Alice is cautious about her privacy and does not want any third party to trace her paths—she is only willing to contribute to uSafe if her privacy is respected. For example, she does not want her identity to be associated with her reports or the locations she has visited. Therefore, she first personalizes her privacy preferences using the interface presented in Fig. 1(c). She opts to use periodic pseudonyms instead of a unique ID (e.g., her real identity or a pseudonym) for the transmission of her reports to the application. The utilization of periodic pseudonyms breaks the link between her successive contributions, and thus prevents the inference of her real identity based on an analysis of her contributions. Alice then authorizes uSafe to send her reports to the application server in a real-time manner by selecting the live reporting option. However, Alice decides not to reveal her exact position when she submits a new report. Instead of her actual coordinates, she chooses to only provide a cloaked position, and selects 100 meters as cloaking parameter. This means that her position will be reported as a square of 100 meters on each side, in which her actual position is included. After this personalization, Alice starts submitting privacy-protected reports about places she encounters during, e.g., her commutes, shopping tours, or

Table 1: Demographics of the participants (n_{total}=183)

Nationality	n	Current occupation	n	Field of occupation	n
German	118	Master student	51	Electrical engineering	72
French	12	Bachelor student	50	Computer science	55
Spanish	10	PhD student	47	Biology	9
Pakistani	8	Postdoctoral researcher	16	Physics	7
Indian	7	Technical staff	7	Mathematics	5
Italian	3	Administrative staff	5	Psychology	4
Other	25	Other	7	Other	31

visits to entertainment centers. For each report, and despite the use of periodic pseudonyms, Alice receives a reward, whose value depends on the degree of granularity of the provided information. She can use this reward to obtain reduced rates for public amenities, such as discounts for the opera or the public swimming pool.

3. Evaluation of the uSafe Application

We have performed a questionnaire-based study to evaluate the concept and design principles of uSafe by interviewing potential users. We recruited the participants by posting announcements on multiple mailing lists and forums at our university, as well as partner universities in France and Spain. As a result, 183 participants anonymously answered our online questionnaire. In this section, we present the outcomes of our study.

3.1. Demographics

The participants were predominantly male (n=122) and aged between 18 and 50 (m=26, SD=6). Table 1 illustrates the distribution of the most represented nationalities, current occupations, and fields of occupation among the participants. In total, the participants came from 24 different countries and showed a high profile diversity including fields of occupation such as mechanical engineering, arts, and linguistics. Most of the participants live (n=88) and work (n=125) in Darmstadt, followed by Frankfurt (n=13 and n=14), Paris (n=9 and n=9), and Madrid (n=8 and n=8).

3.2. Personal Experience

We first asked the participants if they "had already felt unsafe when walking in the city". Among the 183 participants, 44 female (72% of the females) and 76 male (62% of the males) participants reported to have perceived this feeling. We particularly considered this subset of 120 participants and further examined their personal experience. 68% of the 120 participants perceive this feeling on an irregular basis, while it only happened once for 9% of the participants. The remaining participants feel unsafe at the following approximative frequency: daily (3%), monthly (12%), and yearly (8%). Fig. 2 illustrates at which periods of the day these participants feel the most unsafe. The results show that most of the participants start feeling unsafe in the evening, and that this feeling persists until early in the morning with a peak late in the night. Next, we proposed a list of possible reasons to the participants that may have triggered their feelings of being unsafe. Fig. 3 summarizes the results and shows that the three most-cited reasons are the presence of drunken people, dark streets, and menacing people.

3.3. uSafe from a User's Perspective

In the next step, we described the uSafe application and its principles to the 183 participants of our study by adopting the perspective of a potential user. We refer to *user* as a person who consults or benefits from the information provided by others and we identify *contributor* as a person who provides information in form of safety reports. Note that we adopt the latter perspective in Section 3.4. Based on the description of the application, we have examined the interest of the interviewed participants in using uSafe in

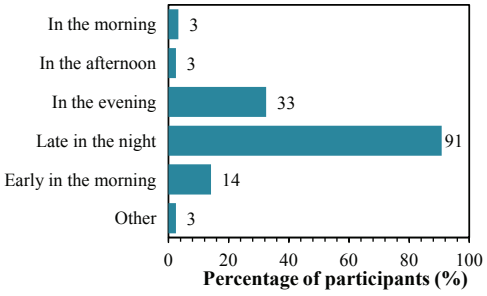


Figure 2: Periods of the day at which the participants felt unsafe (multiple choices possible)

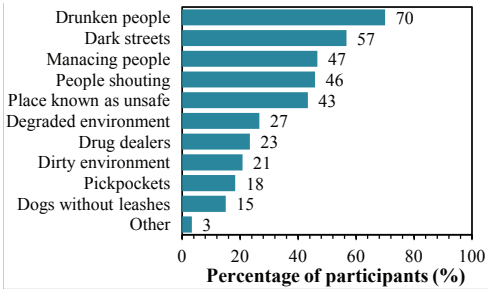
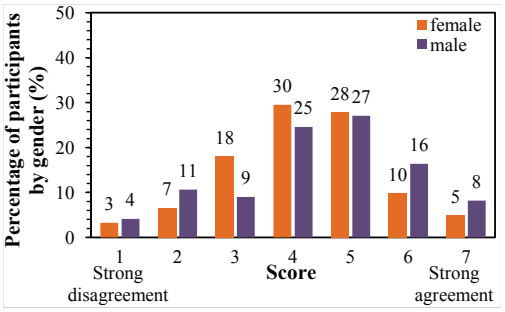
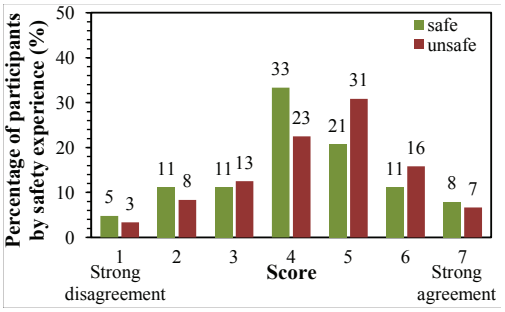


Figure 3: Reasons given by the participants to explain their feeling of unsafeness (multiple choices possible)



(a) Distribution of the answers by gender



(b) Distribution of the answers by safety experience

Figure 4: Impact of gender and safety experience on the interest in using uSafe

general and using the *safety hint* feature in particular, which alerts users when they are about to enter areas rated as unsafe.

3.3.1. Interest in Using uSafe

Firstly, we proposed the following statement to all 183 participants: "I would appreciate using the uSafe application". We evaluated their degree of agreement with this statement using a seven point Likert scale. A score of 1 indicates strong disagreement, 4 is neutral, and a score of 7 indicates strong agreement. As a result, 48% of the participants stated that they would appreciate using uSafe by selecting scores between 5 and 7, while 25% would not appreciate it. The remaining participants remained neutral by choosing a score of 4. In particular, we investigated whether the gender of the participants has an influence on their answer. Fig. 4(a) shows the distribution of the answers by gender. The median rank of the women is equal to 87.26, while the median rank of the men is equal to 94.37. A Mann-Whitney U test shows, however, that the gender difference is not significant (U=3432.000, Z=-0.875, p=0.382, r=0.064). Furthermore, we analyzed whether participants having already experienced a feeling of being unsafe (referred to as *unsafe*) would be more interested in using uSafe than those who never have experienced this feeling (referred to as *safe*). Fig. 4(b) illustrates the distribution of the answers by safety experience. The median ranks of the *unsafe* and *safe* participants are equal to 95.35 and 85.62, respectively. Again, a Mann-Whitney U test shows that the difference in the answers of both groups of participants is not significant (U=3378.000, Z=-1.208, p=0.227, r=0.089). In summary, neither the gender nor the safety experience significantly influence the inter-

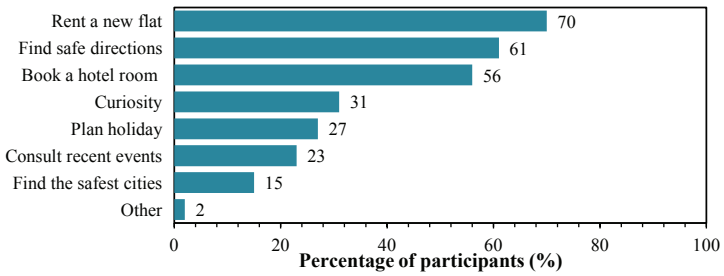


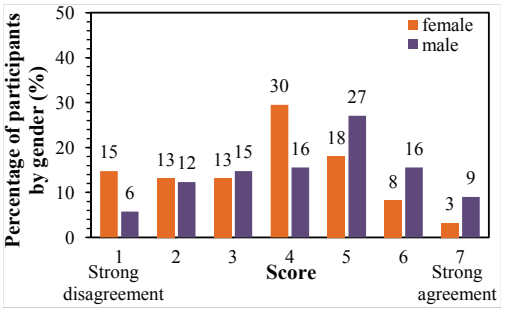
Figure 5: Situations in which the participants would like to use the uSafe application (multiple choices possible)

est of the participants in using the uSafe application.

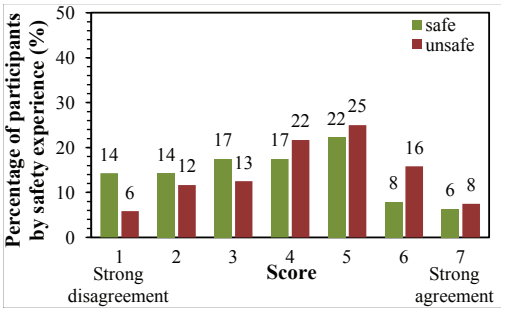
Secondly, we analyzed situations, in which the participants would like to use uSafe. The majority of the participants would be interested in using uSafe when (1) searching for a new flat to rent in order to find an appropriate area, (2) going to a place they have never been and searching for the safest directions, and (3) booking a room in a hotel in order to know how safe the area is, as illustrated in Fig. 5. This especially highlights interest in uSafe for areas unfamiliar to the participants. We finally observed that 73% of the participants "would be interested in knowing why other users have felt unsafe". The majority of the participants is therefore not only interested in knowing if an area is safe, but also in knowing the reason(s) behind the rating—a feature readily supported by uSafe.

3.3.2. Safety Hints

We examined whether the participants of our study "would like being alerted by [their] mobile phone when [they are] about to enter areas rated as critical or unsafe by other users". According to the results collected using a seven point Likert scale, 45% of the participants would dislike to be informed (including 22% who would strongly dislike it), while 46% would like it. Since the opinion of the participants is clearly divided into two groups, we decide to maintain the safety hint feature in our prototype implementation as an optional feature in order to allow users to individually activate/deactivate it. Nevertheless, 56% of the participants found that "a personalized vibration of [their] mobile phone is an unobtrusive and appropriate solution to alert [them] if [they] are about to enter a critical or unsafe area".



(a) Distribution of the answers by gender



(b) Distribution of the answers by safety experience

Figure 6: Impact of gender and safety experience on the interest in contributing to uSafe

3.4. uSafe from a Contributor's Perspective

After having adopted the perspective of potential users in Section 3.3, we evaluate uSafe from the perspective of potential contributors to the application. We first analyzed the general interest of the participants in contributing to the application by reporting their safety feelings and giving reasons for such feelings. For this analysis, we used a seven point Likert scale and proposed the following statement to the participants: "I would be ready to contribute to the uSafe application by reporting my safety feelings and giving reasons of such feelings". 44% of the participants agreed with this statement, whereas 36% disagreed. Additionally, Fig. 6(a) and 6(b) present the distribution of the answers of the participants by gender and by safety experience, respectively. We first investigated the impact of gender on the answer of the participants. Male participants show a median rank of 98.80, while female participants show a median rank of 78.40. A Mann-Whitney U test confirms that male participants would be significantly more ready to contribute to uSafe than female participants (U=2891.500, Z=-2.494, p=0.013, r=0.184). While the test shows a significant difference between gender, the effect size is, however, small to medium. Next, we analyzed the influence of the safety experience of the participants on their answer. The median ranks of the *unsafe* and *safe* participants are equal to 98.02 and 80.53, respectively. A Mann-Whitney U test shows that the difference between both groups of participants is significant, i.e., the participants having already felt unsafe would be significantly more ready to contribute to uSafe (U=3057.500, Z=-2.155, p=0.031, r=0.160). Again, the effect size remains small to medium. Furthermore, 34% of the participants "would prefer reporting [their] safety feeling in real-time

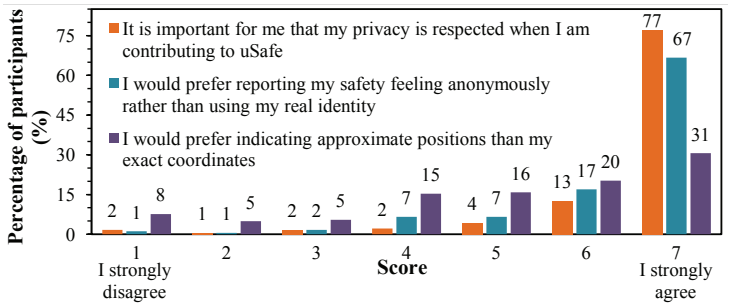


Figure 7: On the importance of privacy for the participants and their preferences in terms of anonymity and location cloaking

rather than afterwards", while 42% would prefer using retrospective reports and 24% remained neutral. Our participants thus have a slight preference for contributing retrospective reports compared to live reports. Moreover, participants ready to contribute to uSafe indicated which safety threats they would like to report in a free text field. Five main safety threats were identifiable in their answers: dark streets (n=21), drinking/drunken people (n=11), aggressive people (n=9), areas where drugs are usually sold/consumed (n=8), and deserted places (n=3).

Asked if they "would be more motivated to contribute to uSafe if [they] would obtain a reward for each contribution", 38% of the participants disagreed and 36% agreed, whereas 26% remained neutral. However, only 20% of the participants "would be ready to provide additional information about, e.g., [their] current location or [their] identity in exchange for additional rewards", while 63% would not trade personal information for rewards. Both results highlight that the participants are conscious of privacy implications and that a loyalty program is expected to slightly encourage their participation in uSafe. Among the different rewards we proposed, "vouchers" would motivate 43% of the participants to contribute more, while the "access to additional features and functions of uSafe" and to "be listed among the most contributing users" would motivate 31% and 11% of the participants, respectively (multiple choices possible).

3.4.1. Privacy Concerns

Since uSafe has been designed with a focus on privacy, we addressed this topic in our questionnaire specifically. The participants confirmed that privacy is a determinant factor in their decision to contribute to an application.

Among the participants, 94% stated that "it is important for [them] that [their] privacy is respected when [they are] contributing to uSafe" as shown in Fig. 7. In particular, 90% of the participants "would prefer reporting [their] safety feelings anonymously rather than using [their] real identity". In uSafe, users can freely decide to utilize a unique username/pseudonym or periodic pseudonyms in order to enhance the protection of their anonymity further. In comparison, the participants seem to be less willing to cloak their locations than to use pseudonyms, as only 67% "would prefer indicating approximate positions than [their] exact coordinates" by means of cloaking mechanisms.

The differences between the first statement made by the participants, that their privacy is important, and their preferences in applying privacy-preserving mechanisms highlight the fact that the participants do not fully associate anonymity and/or location privacy with their own definition of privacy. Otherwise, the distribution of the scores would have been identical for the three questions. Also, it confirms the diversity of personal privacy conceptions between participants.

In summary, the study has shown that the participants would be ready to use and contribute to uSafe. This result has been confirmed by the comments left by the participants, e.g., "I like your idea!", "It can be a pretty handy application.", "This whole uSafe thing seems really interesting to me, great approach!", and "I strongly recommend you to carry on this project".

4. uSafe Architecture and Prototype

In this section, we present the architecture of the uSafe application. Its concept and design principles have been evaluated by the participants of the aforementioned questionnaire-based study. We provide an overview of the architecture, before describing the underlying mechanisms and providing details about our prototype implementation. In particular, we discuss how the uSafe architecture protects the location privacy and anonymity of the users—a feature stated as important by 94% of the participants of our questionnaire-based study.

4.1. Architecture Overview

The uSafe application is centered on the creation, processing, visualization and utilization of safety reports. A safety report includes a safety feeling, i.e., the degree of safety perceived by the user, optionally the reason(s) behind

this feeling, and the corresponding spatiotemporal information, i.e., location and collection time. The architecture of the uSafe application is comprised of mobile clients, an application server, and a third party called the *reward and pseudonym manager* (RPM), as illustrated in Fig. 8. The client application fulfills two fundamental functions. Firstly, it allows the users to create safety reports. Depending on the privacy preferences of the users, the reports can be transmitted using either a unique identifier (i.e., the real identity of the user or a pseudonym) or periodic pseudonyms generated in collaboration with the RPM. Secondly, the client application caters to the visualization of the collected safety reports in the form of heat maps, and offers a safety-aware navigation function as well as a safety hint function, which alerts the users when they enter areas rated as dangerous by other participants. In our prototype, Android Nexus S mobile phones serve as clients.

The clients submit the created safety reports to the application server, where they are collected and consolidated. Local maps are periodically updated according to the latest received reports in order to reflect the average safety feeling per geographical area. In addition to the compilation of maps, the application server attributes a reward score for each transmitted report to the corresponding user. Reward scores are calculated based on the degree of granularity of the information provided. The finer the degree of granularity is, the greater the reward. The application server finally transmits the attributed reward scores to the RPM, which maintains a reward account for each client. Both application server and RPM have been realized using Apache Tomcat servers in our prototype implementation.

In the remainder of this section, we describe the functions of the individual components as well as their interactions.

4.2. Reporting Mechanisms

The following steps are performed for each report: (1) report creation, (2) report transmission, (3) report processing, and (4) report visualization and utilization. We discuss each step in detail in the following.

4.2.1. Report Creation

Users can choose to create either live reports or retrospective reports using the application running on their clients. In live reports, the users report their safety feeling and comment on events in real-time. They can choose to generate either discrete or continuous reports. In order to create discrete live

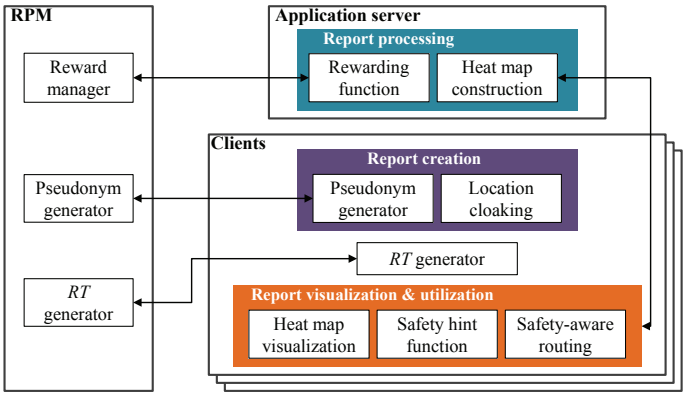
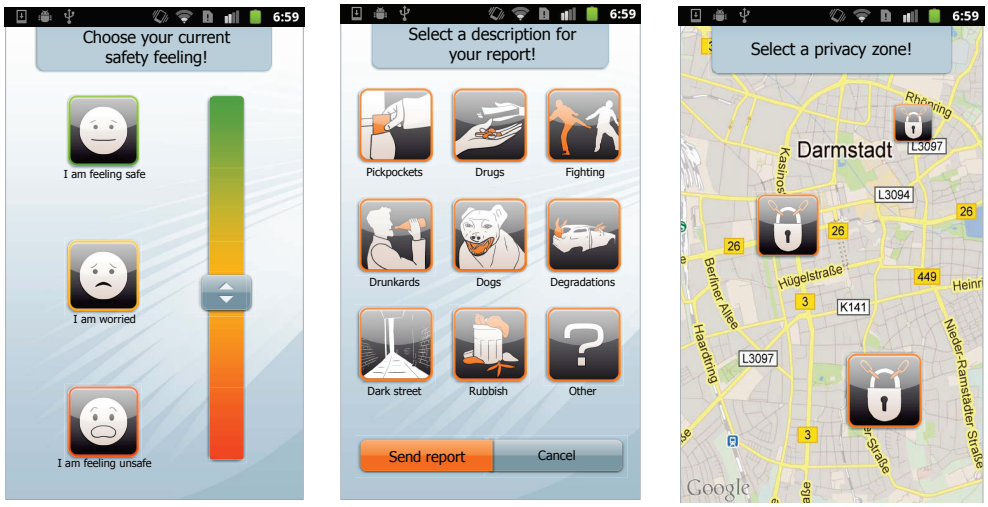


Figure 8: uSafe architecture

reports, each user selects her current safety feeling among the following options: "I am feeling safe", "I am worried", or "I am feeling unsafe", using the interface shown in Fig. 9(a). Then, she can indicate reason(s) for such feeling by selecting the appropriate icon in the interface illustrated in Fig. 9(b) or by writing a personal comment. After both the safety feeling and its reason have been selected, the client retrieves the current position of the user and applies the privacy rules defined by the user. Privacy rules are applied to protect the privacy of the user when creating a safety report. In absence of protection mechanisms, the application managers and other users have access to the exact location she visited. In addition to endangering her location privacy, additional information may be inferred, such as her political view and her medical condition if she indicated her safety feeling close to a political event and a hospital, respectively. The threats to her privacy increase with the number of created safety reports, as they provide more and more information about her behavior. Even if she is using a pseudonym as username, her identity may be inferred based on an analysis of her frequently visited locations, such as her domicile and workplace locations. Once the address of her domicile has been identified, a reverse white pages lookup may reveal her real identity as shown in [10]. In order to protect her location privacy and anonymity, uSafe proposes the utilization of three main mechanisms: (1) location cloaking, (2) privacy zones, and (3) periodic pseudonyms (see Section 4.2.2). Using location cloaking, the user can select to what degree of granularity her location is released. Depending on the selected degree of granularity, the client utilizes different grid overlays with cell sizes equal to



(a) Selection of perceived safety feeling

(b) Selection of reason for safety report

(c) Example of privacy zones

Figure 9: Selected screenshots of user interface elements

the selected side length, in order to replace the exact coordinates of the user by the ID of the corresponding sector. Note that each overlay divides the map into sectors of equal size, but the size varies depending on the selected overlay. For example, our implementation includes a hierarchy of 3 overlays with sector sizes of 100, 500, and 2,000 meters, respectively. The users can also define privacy zones as illustrated in Fig. 9(c), in which their location should not be released to the application server without their consent.

In order to report over larger and safe areas, the users can decide to generate continuous reports. Compared to the discrete reports, the users only select their current safety feeling (without indicating any reason) and the clients periodically generate a report including the same safety feeling until the user modifies her feeling or stops the reporting. In the absence of user interactions, the generation function is deactivated after a certain time.

The same privacy rules are applied to the location information embedded in the continuous reports as in the discrete reports. Using retrospective reports, the users can comment on events they observed in the past and retrospectively indicate their safety feelings. Therefore, the client records and stores the paths followed by the corresponding user during the day. At the end of the day, the user can browse her path and manually annotate locations she visited with her experienced safety feelings. The default degree

of granularity, at which the location of each report is released, is defined by the user using the privacy interface, but it can also be manually modified. After the creation of the reports, the user can decide to either conserve her traces or discard them. Uncommented paths are automatically erased from the clients after an expiration time defined by the user.

4.2.2. Report Transmission

The completed reports created by the users on their mobile phones are then transmitted to the application server. In our prototype, the clients mainly communicate with the application server via Wi-Fi/3G using HTTPS, and we assume that the interactions of the clients with the application server are anonymized using, e.g., disposable IP and MAC addresses or anonymous communication networks [11]. For the transmission of the reports, the users can select to utilize the identity associated with their uSafe account (i.e., their real identity or a username) or periodic pseudonyms. In the former case, a unique identity is associated to all reports transmitted by the users to the application server. This poses the risk that their real identity and sensitive personal information can be inferred based on the location information contained in the reports as detailed in Section 4.2.1. In order to preserve their anonymity, the users can opt to transmit their reports using periodic pseudonyms. Instead of being linked to a permanent pseudonym, the transmitted reports are linked to the current pseudonym of the user for the duration of validity of the pseudonym, i.e., its period. In other words, only the reports transmitted during the same period are associated to a unique pseudonym. The real identities of the users thus become harder to infer since the location information about the users are split among multiple pseudonyms.

In our prototype, the generation of the periodic pseudonyms is based on the *IncogniSense* framework we presented in [12]. Instead of attributing reputation scores to the users based on the quality of the reported sensor readings, we integrate elements of this framework to attribute rewards to the users for their contribution while supporting their anonymity. The clients generate the periodic pseudonyms in collaboration with the RPM using RSA blind signatures [13]. The utilization of blind signatures ensures the authenticity of the pseudonyms without revealing them to the RPM and prevents the RPM from linking the pseudonyms to the identity of the clients. Moreover, our implementation guarantees that the clients have only one active pseudonym per period and hinders potential Sybil attacks. These attacks can be launched by malicious clients trying to fraudulently augment their

reward by transmitting the same report using multiple pseudonyms in the same period of time. The underlying mechanisms are implemented as follows.

Each client is registered with the RPM and has a permanent identifier ID and a permanent private/public key pair associated with its ID. The RPM generates new private/public pair of keys for each period of time. Each period of time T corresponds to the period of validity of the pseudonyms and is common to all clients, i.e., the clients simultaneously change their pseudonyms at the beginning of T. In order to generate a new pseudonym for the next period of time, each client follows the subsequent steps. First, the client generates a private/public key pair for the new pseudonym and adopts its modulus as its new pseudonym referred to as P. Next, the client generates the signature of P by interacting with the RPM. The client first prepares a message m_P using the public key of the RPM valid for T and signs it with its permanent private key to guarantee its authenticity. Then, the client transmits its ID, the prepared message m_P, its signature, and the interval of validity T for P to the RPM for blind signature. The RPM verifies the authenticity of m_P, and that the client has no existing pseudonym for this interval, before generating a blind signature signing m_P. The client finally generates the pseudonym's signature from the blind signature, which completes the generation of the pseudonym P. Next, the client transmits the reports created by the corresponding user to the application server using the pseudonym valid for the current period of time. For multiple retrospective reports, the clients distribute the reports among different consecutive pseudonyms to avoid their association to a unique identity.

4.2.3. Report Processing

The reports transmitted by the clients are first stored in a database on the application server that periodically analyzes the incoming reports in order to: (1) construct/update the heat map and (2) attribute reward scores to the clients for their contribution. For the heat map construction and updates, the application server first periodically considers the newly received safety feelings and transforms each of them into a numerical value. Without loss of generality, the safety feelings "I am feeling safe", "I am worried", and "I am feeling unsafe" are replaced in our prototype implementation by the value 0, -50, and -100, respectively. Next, the application server utilizes the same grid overlays as those utilized by the clients to cloak the location of the users (see Section 4.2.1) in order to identify which sector(s) are concerned by each new report. Since the overlays are identical, the application server can easily

(a) Sector size of 100 m (b) Sector size of 500 m (c) Sector size of 2 km

Figure 10: Example of overlays with different degrees of granularity

credit the sector(s) with the numerical value corresponding to the safety feeling and compute the new average value for the concerned sector(s). The average value is then translated into one of the five colors, which range from green for safe sectors to red for unsafe sectors. The operation is repeated for all sectors across the different overlays, such that the users can later navigate across the different overlays by zooming in and out from the map and observe the heat map with different degrees of granularity as shown in Fig. 10.

Furthermore, the application server analyzes the transmitted reports in order to attribute reward scores to the corresponding clients. The value of the attributed reward score depends on the degree of granularity of the provided information. In our prototype implementation, the application server attributes a score of value 20 to live reports providing information in real-time, while it attributes a score of 10 to retrospective reports, since the reports describe past events. Additional reward scores are attributed depending on the selected level of location cloaking. By embedding their exact position in the report, the users gain an additional score of 20, whereas they gain only a reward of 15, 10, or 5 when they select to indicate their position using a square of size 100, 500, and 2,000 meters, respectively. Note that the selected values for the reward scores only serve as example and can be easily modified to cover diverse rewarding strategies. Next, the application server transmits

the reward scores with either the unique identifier of the users or their current periodic pseudonym to the RPM, which maintains a reward account for each identifier and pseudonym. The RPM then credits the reward account of each user from the attributed reward score(s). Users using periodic pseudonyms can collect their accumulated reward scores using their current or past pseudonyms. The collection process is realized using *reward tokens* (RTs), which are generated by the clients in collaboration with the RPM, and are based on blind signatures. The utilization of blind signatures prevents the RPM from linking the client's identity with its pseudonyms. Since the RPM is involved in the collection process, our implementation prevents the clients from corrupting their reputation. The collection of the reward scores by the clients is also part of our *IncogniSense* framework [12], but differs in the sense that the clients do not need to transfer their rewards from their current pseudonym to the next. Instead, the clients can collect their rewards at any time, using either their current pseudonym or one that has already expired according to the following steps. The client first requests the value of the reward account of the corresponding pseudonym, e.g., its current pseudonym $P_{current}$, from the RPM. The generation of each RT is comparable to the generation of a pseudonym, except that the client does not generate any key pair and both client and RPM use different key pairs for the blind signatures. These key pairs are generated by the RPM in the bootstrapping phase and each private/public key pair is associated with a reward value and determines the reward score associated with a given RT. For each created RT, the client selects a random bit string as an identifier for the RT and prepares the message m_{RT} for blind signature using the public transfer key corresponding to the RT's value. The client signs m_{RT} using the private key of $P_{current}$. The real identity of the client is hence not revealed while collecting the reward score R_{score}. The client transmits $P_{current}$, R_{score}, m_{RT}, and its signature, to the RPM for blind signature. The RPM verifies that m_{RT} is used for the first time as well as the balance of the reward account of $P_{current}$ before decrementing it by R_{score}. After verification, the RPM blindly signs m_{RT} with the corresponding private key. Finally, the client uses the blind signature to generate the final signature of the RT. Depending on the selected rewarding program, the users can trade their RTs to gain access to additional features of uSafe, or be listed in the hall of fame of the most contributing users. The traded RTs are finally marked as used in order to prevent their reuse.

4.2.4. Report Visualization and Utilization

The users can consult the heat map constructed by the application server on their client. In addition to an automatic daily update of the lower overlay, the users can manually trigger it from the menu. The higher overlays are locally constructed by the clients. The construction of the local heat map supports both the safety-aware navigation and safety hint functions. For the safety-aware navigation function, the clients request directions between two locations using the Google Directions API [14] and compute the average degree of safety for each returned alternative. For the safety hint function, the clients monitor the average degree of safety of the sector in which they are currently moving. If a given threshold is reached, the clients vibrate according to a customizable pattern. Additional features could be integrated to our prototype implementation, such as an indication of nearby public transport stations as alternative solutions for optimally edging zones rated as unsafe. The concept of safety rating could then be extended to public transport. For example, the users could rate the bus they travelled in, and other users could use this rating to decide which bus line is the safest for their route. We, however, consider these extensions as future work.

5. Discussions and Open Issues

In addition to positive feedback, participants of our study have raised two specific issues, which we address in this section.

5.1. Trustworthiness and Reliability of the Reported Information

One participant remarked that "The idea is good but is prone to fake entries". By definition, a feeling of safety is subjective. This feeling can be influenced by different factors, such as age, gender, personal experience, or physical conditions. It is therefore difficult to distinguish honest from falsified reports. Existing reputation systems, e.g., [15], remain inefficient in coping with this issue because they are tailored to systems collecting factual information, such as noise level measurements. The same problem already exists, however, in applications based on user-generated reviews (see Section 6). For example, restaurant owners may serve their own interests by writing or soliciting praising reviews about their own restaurants. The fraud may only come to light if honest participants report negative experiences, which negatively impact the rating initiated by the malicious owners. The

more honest reviews, the more reliability. The ratio between honest and malicious users cannot be controlled at an application level, though. Means such as moderators, voting mechanism, or cross-verification with multiple sources of information (e.g., local newspapers) may help to improve the reliability of information, but cannot guarantee it due to the subjective nature of the reported information and the inherent openness of the application.

5.2. Impacts of the Rating on the Area Frequentation and the Users

One participant commented: "I fear this kind of application can create a real discrimination between areas". The primary objective of uSafe is to provide information to the users about events or locations, where their safety may be endangered. uSafe does not provide means to physically thwart the safety threats, but means to edge them based on the reports of others. While edging unsafe areas may protect the safety of the users, it may also favor the decay of these areas. However, citizens feeling unsafe in an area may also naturally avoid it afterwards without even needing to consult uSafe. This vicious circle can only be broken if a common effort is undertaken by public bodies and citizens, in which the city councils were to work in synergy with the police and local organizations to find appropriate solutions. In this scenario, uSafe could provide a wealth of information to, e.g., social workers and urban conflict managers, by pointing out areas requiring particular attention.

Another participant concluded that "It can happen that people become more afraid when using this application". Since the potential threats are reported, they become visible and may modify the perception of the user about her environment. Instead of only relying on her own experience of the city, the user gains access to the experiences shared by others, which refines the granularity of the picture initially drawn. This may either reassure her, if she was witness to a punctual safety threat, or reinforce her feeling of being unsafe. Such impact should be measured using a long-term user study in which participants would be using uSafe in their everyday life over several months. We, however, consider this study as future work.

6. Related Work

The design of the uSafe application has been influenced by two main types of existing applications. uSafe was first inspired by existing participative applications, in which users contribute self-generated content such as

ratings and reviews to the application, and also by applications that provide safety-oriented information to the users. In this section, we present these applications and discuss their differences from the uSafe application.

A plethora of online applications based on ratings and reviews written by users about a particular topic have emerged. For example, more than 1.9 million reviews have been posted in *Qype* [16] about restaurants, doctors, or other available services. Additionally, the *foursquare* application [17] counts a community of more than 10 million users who can share their experiences by indicating their current location to the application. Both the number of Qype reviews and the size of the community in foursquare show an increasing interest from the public in contributing self-generated content, and have motivated our decision to make uSafe a participative application. This decision has been further reinforced by the existence of different initiatives for which users report about their direct urban environments. For example, users can rate the quality of their surroundings using *RateMyArea.com* [18], or they can post pictures of garbage to evaluate the effectiveness of the recycling process on the UCLA campus using the *GarbageWatch* project [19, 20]. These initiatives, however, mainly concentrate on the cleanliness of the environment or the quality of the public infrastructure, and do not address the aspect of safety. In the domain of safety, *Ushahidi* [21] shares a number of similarities with uSafe since the project was launched to map citizen reports of violence during the Kenyan crisis in 2008. It, however, does not consider the feeling of safety of the users and does not support certain features, such as safety-aware routing planning and safety hints. In summary, uSafe was inspired by existing participative applications, but uSafe either differs in the subject of study or offers additional functions unavailable from these applications.

On the other hand, the design of uSafe has been influenced by existing safety-oriented applications. These applications are, however, not based on user-generated content. For example, police departments directly provide information to the public about crimes and policing through *POLICE.uk* [22] and *My Neighborhood Map* [23]. Instead of user-generated content, *SpotCrime* [24] and *CrimeMapping.com* [25] exploit, respectively, published news releases and records from law enforcement agencies to build maps displaying crime information for the public. As in these applications, uSafe displays safety information on heat maps, but the information sources are different and uSafe provide additional features.

Consequently, uSafe can be seen as the first application that addresses the safety of the citizens in a participative manner and, furthermore, provides

privacy-aware mechanisms absent in the above applications.

7. Conclusions

We have proposed a privacy-aware and participative application for citizen safety in urban environments called uSafe. uSafe is based on user-generated reports about their feeling of safety when they travel in the city. The reported safety feelings can benefit multiple entities, ranging from the users themselves to, e.g., city councils. We have evaluated the concept of uSafe by conducting a questionnaire-based study involving 183 participants who validated the utility of such application. The participants confirmed that they would use the presented application in different scenarios. Additionally, the results show that almost all participants are concerned about their privacy and that only a minority would trade private information against potential rewards. Moreover, we have presented the uSafe architecture and provided details about our prototype implementation. While the uSafe application has been presented in isolation in this article, we plan to integrate and extend it with additional urban applications in order to increase the degree of granularity of the drawn portraits of the urban environments.

Acknowledgment

The authors would like to thank the participants of the study as well as Andreas Reinhardt and Kai Trumpold for the fruitful discussions. Our thanks also go to the anonymous reviewers for their valuable comments and suggestions. This work was partially supported by CASED (`www.cased.de`) and by a grant of the European initiative EIT ICT Labs (`http://eit.ictlabs.eu`) in the thematic action line "Digital Cities of the Future".

References

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M. Srivastava, Participatory Sensing, in: Proceedings of the 1st Workshop on World-Sensor-Web (WSW), 2006, pp. 1–5.

[2] A. Campbell, S. Eisenman, N. Lane, E. Miluzzo, R. Peterson, People-centric Urban Sensing, in: Proceedings of the 2nd Annual International Wireless Internet Conference (WICON), 2006, pp. 18–31.

[3] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, P. Boda, PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research, in: Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2009, pp. 55–68.

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

[5] R. Rana, C. Chou, S. Kanhere, N. Bulusu, 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), 2010, pp. 105–116.

[6] P. Mohan, V. Padmanabhan, 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), 2008, pp. 323–336.

[7] Federal Criminal Police Office, Police Crime Statistics Yearbook 2009 - Abridged Version, Online: `http://www.bka.de` (accessed in 11.2011).

[8] K. Sheehan, M. Hoy, Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns, Journal of Advertising 28 (3) (1999) 37–51.

[9] D. Christin, Impenetrable Obscurity vs. Informed Decisions: Privacy Solutions for Participatory Sensing, in: Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications (PerCom Workshops), 2010, pp. 847–848.

[10] J. Krumm, Inference Attacks on Location Tracks, in: Proceedings of the 5th IEEE International Conference on Pervasive Computing (Pervasive), 2007, pp. 127–143.

[11] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, N. Triandopoulos, AnonySense: A System for Anonymous Opportunistic Sensing, Journal of Pervasive and Mobile Computing 7 (1) (2010) 16–30.

[12] D. Christin, C. Roßkopf, M. Hollick, L. Martucci, S. Kanhere, IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications, in: Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications (PerCom), 2012, pp. 135–143.

[13] D. Chaum, Blind Signatures for Untraceable Payments, in: Advances in Cryptology: Proceedings of Crypto 82, 1983, pp. 199–203.

[14] The Google Directions API, Online: `http://code.google.com/intl/en/apis/maps/documentation/directions` (accessed in 11.2011).

[15] K. Huang, S. Kanhere, W. Hu, Are You Contributing Trustworthy Data?: The Case for a Reputation System in Participatory Sensing, in: Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM), 2010, pp. 14–22.

[16] Qype, Online: `www.qype.com` (accessed in 11.2011).

[17] Foursquare, Online: `https://foursquare.com` (accessed in 11.2011).

[18] RateMyArea.com, Online: `www.ratemyarea.com` (accessed in 11.2011).

[19] S. Reddy, D. Estrin, M. Srivastava, Recruitment Framework for Participatory Sensing Data Collections, Pervasive Computing 6030 (2010) 138–155.

[20] GarbageWatch, Online: `www.garbagewatch.com` (accessed in 11.2011).

[21] Ushahidi, Online: `http://ushahidi.com` (accessed in 11.2011).

[22] POLICE.uk, Online: `http://www.police.uk` (accessed in 11.2011).

[23] My Neighborhood Map, Online: `http://web5.seattle.gov/mnm/policereports.aspx` (accessed in 11.2011).

[24] SpotCrime, Online: `http://spotcrime.com` (accessed in 11.2011).

[25] CrimeMapping.com, Online: `www.crimemapping.com` (accessed in 11.2011).