PriPref Broadcaster: Enabling Users to Broadcast Privacy Preferences in Their Physical Proximity

Bastian Könings,[1] Sebastian Thoma,[1] Florian Schaub,[2] Michael Weber[1]

[1]University of Ulm
Ulm, Germany
[firstname.lastname]@uni-ulm.de

[2]Carnegie Mellon University
Pittsburgh, PA, USA
fschaub@cmu.edu

ABSTRACT

While privacy is often treated as an information centric issue, privacy issues in ubiquitous and mobile computing also encompass physical or territorial aspects, i.e., the right to be left alone or undisturbed. Disturbances that affect privacy often stem from persons nearby and their mobile devices, e.g., ringing phones, loud phone calls, or sounds of mobile games. We propose *PriPref Broadcaster*, a smartphone-based approach for communicating personal privacy preferences to persons in physical proximity. Our approach further supports automatic adaptation of mobile device settings based on the dominating preferences in the current environment. Results from a usability study and a five-day field trial with 28 participants show that broadcasting privacy preferences is perceived as meaningful and has the potential to support privacy signaling in many everyday situations.

Categories and Subject Descriptors

K.4.m [**Computers and Society**]: Privacy; H.5 [**Information Interfaces and Presentation**]: Prototyping, mobile HCI

Keywords

Privacy preferences; privacy signaling; mobile devices;

1. INTRODUCTION

Privacy in relation to technology is mostly considered an information-centric issue with respect to Westin's [45] popular privacy definition. However, it also involves physical aspects of territorial privacy which can be defined as *"one's right to be physically left alone or undisturbed"* [41]. These aspects are also reflected in Altman's [1] notion of solitude as *"control over where one directs one's attention and how one controls distraction"* [5].

Nowadays, typical causes of undesired disturbances are nearby persons and their mobile devices, e.g., loud conversations [14], phone calls [37, 15], or annoying ringtones [22]. In such situations, it is usually inconvenient or awkward to signal personal privacy preferences to such disturbers. For instance on a train, if one would prefer quietness to work or sleep and others are being noisy, one must directly approach the disturbers, which may cause socially awkward or unpleasant situations.

Such privacy-related disturbances do not only exist in public places and situations but also in more familiar situations and places, such as the work place. Several studies [8, 12, 3, 13] have shown that disturbances in open-plan offices reduce employees' satisfaction and perceptions of privacy, especially in terms of visual and acoustic privacy [13].

In this work, we propose the concept of broadcasting user-defined privacy preferences (PriPref) in one's physical proximity as an approach to express privacy preferences in an anonymous way without requiring to confront the respective disturber. For this purpose, we developed smartphone-based privacy signaling mechanisms leveraging WiFi and Bluetooth. We implemented these signaling mechanisms in our mobile app *PriPref Broadcaster*. PriPref Broadcaster allows users to create profiles for different situations, broadcast their preferences when desired, and learn about the privacy preferences of other present persons. PriPref Broadcaster further supports the automatic adaptation of phone settings according to the dominant preferences in the current environment, for example, switching to "vibrate only" if the majority of other persons signal a need for quiet.

We conducted an online survey with 101 participants to elicit common sources of everyday disturbances and in which situations they occur. From the results, we derived the most relevant disturbances participants wanted to reduce in everyday situations, e.g., at work or on the bus or train. These disturbances determined the types of privacy preferences supported by PriPref Broadcaster. We evaluated PriPref Broadcaster in preliminary usability experiments (n=10) and a five day field trial with 28 participants. Our results show that signaling privacy preferences in the physical proximity was highly accepted, perceived as meaningful, and used in different everyday situations. Yet, while most participants appreciated it if the phones of other persons would automatically adapt to received privacy preferences, the majority stated that they would not want their own phones to automatically adapt to preferences of others. We discuss the implications of our results on the design of effective privacy signaling mechanisms for physical environments.

After motivating the meaning of disturbances with respect to privacy by discussing different privacy dimension in Sec-

MUM '14, November 25 - 28 2014, Melbourne, VIC, Australia
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-3304-7/14/11…$15.00
http://dx.doi.org/10.1145/2677972.2677978

tion 2, we will discuss related work on privacy signaling and on reducing phone call related disturbances in Section 3. Section 4 outlines the online survey's results which guide the design of PriPref Broadcaster in Section 5, followed by a discussion of our evaluation in Section 6 and future work in Section 7, respectively.

2. PRIVACY DIMENSIONS

In the context of computing systems, privacy is mainly considered an information-centric issue, based on Westin's definition of privacy as *"the claim of individuals [...] to determine for themselves when, how, and to what extent information about them is communicated to others"* [45]. However, controlling the flow of personal information is only one aspect of privacy. From a more traditional point of view, privacy can be understood as *"the more general right of the individual to be let alone"* [44]. This popular definition, given by Warren and Brandeis in the context of the rise of handheld cameras, reflects the fact that privacy is not only about control of personal information but also about solitude [34, 3, 6], control of personal space and *"the selective control of access to the self"* [1].

These aspects are captured in the concept of *territorial privacy* [29], which has been defined as *"one's right to be physically left alone or undisturbed"* [41]. Brey [7] defines disturbances in relation to privacy as *"physical intrusions, in which privacy is violated through physical interventions."* Boyle and Greenberg [5] generalize Altman's [1] definition of solitude as *"control over where one directs one's attention and how one controls distraction."*

In the context of the work place, Brill et al. [8] further classify similar privacy aspects into *"control over accessibility,"* e.g., by visitors or phone calls, and *"control of visual distractions and interruptions."* Birnholtz et al. [3] describe this aspect as the *"control over information moving toward the self (including interruptions)."*

Thus, privacy can be understood as a multi-dimensional construct that involves aspects of information privacy and territorial privacy. Bok [4] defines this multi-dimensional view of privacy in terms of access control as *"the condition of being protected from unwanted access by others – either physical access, personal information, or attention."* Smith [43] also tries to combine both of these dimensions by defining privacy as *"the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."*

While, traditionally, territorial privacy was affected mostly by other persons (e.g., by approaching someone, by making noise, or by conducting loud conversations), the increasing pervasion of technology in our everyday life creates new territorial privacy affecting sources (e.g., ringing phones or other noise from systems and devices in our environment). We propose to address such issues by signaling users' privacy preferences in physical proximity and thus provide a first step towards more privacy-friendly environments.

3. RELATED WORK

Only a small number of existing proposals have considered how users can signal privacy preferences to others. However, there has been some work on managing phone-related interruptions. We discuss relevant related work in both domains.

3.1 Privacy Signaling

Signaling of information-centric privacy preferences has previously been proposed in the web context. The "do not track" HTTP header is intended to communicate advertising opt-out preferences to websites [36]. Privicons [27] are icons that a sender can include in emails to signal recipients how the email should be handled (e.g., "keep secret" or "don't print"). PrivacyJudge [28] combines cryptographic privacy enforcement with privacy icons to support privacy-aware sharing of information in online social networks.

In the mobile and ubiquitous computing domain, privacy beacons have been proposed as an approach to enable ubicomp devices to signal their data practices [31] by sending out respectively encoded wireless messages [30]. However, hardly any work has considered how individuals can be supported in signaling their territorial privacy needs to surrounding ubiquitous computing and mobile devices. One example is the interactive door "Shoji" [32]. It uses colored areas and brightness levels on its surface to signal disturbance-related privacy preferences (e.g., "do not disturb") to roommates in shared apartments. Roesner et al. [40] propose *world-driven access control* to signal privacy preferences to environmental sensors, e.g., video cameras. They suggest to use different signaling mechanisms, such as QR codes, visual markers, or ultrasound for preference communication. QR codes and visual markers are also proposed by the Offlinetags [18] and TagMeNot [9] projects to prevent undesired picture or video recordings. Here the idea is that visual markers are detected by cameras and used, for instance, to blur or mask the user's face in the recorded video stream.

3.2 Managing phone call interruptions

Further research has aimed to reduce interruptions caused by phone calls. Most existing approaches [2, 25, 26, 38] require persons being called to share their own context information (e.g., location, appointments, or activity) with callers in order to inform when to place a call. However, while these approaches can enhance territorial privacy by mitigating undesired disturbances, sharing of one's own context poses a risk for a user's information privacy. This trade-off has already been investigated by Hudson and Smith [20] in the context of computer supported cooperative work.

In contrast to requiring callees to share their context information, Grandhi et al. [17] propose that callers share more detailed information about the reason of their call. Their work is based on their prior findings stemming from the analysis of incoming call acceptance factors [16]. A collaborative approach for call acceptance decisions is proposed by Marti and Schmandt [35] based on wirelessly actuated finger rings. The rings vibrate on each incoming call in a group of conversation partners and each person can veto the call by touching their finger ring.

Other approaches automatically adapt phone settings, e.g., based on calendar information [24]. Phone sensors and wearable sensors have also been used to learn a user's volume preferences for notifications about incoming calls, SMS, and calendar alarms [23, 19, 42, 46].

In contrast to related work, PriPref Broadcaster enables users to signal privacy preferences to others in their proximity without requiring instrumentation of the environment or having to share personal context.

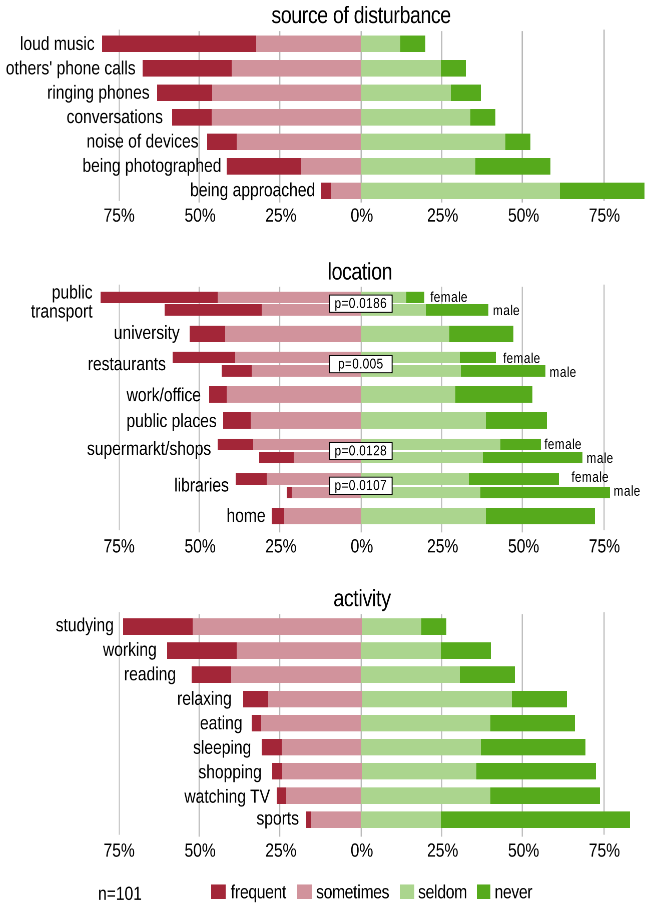


Figure 1: Reported frequency of common sources of everyday disturbances and situations (location and activity) in which they occur. Significant gender specific differences have been found for 4 locations.

4. DISTURBANCES IN EVERYDAY LIFE

In order to determine what privacy preferences would be relevant to consider and support in PriPref Broadcaster, we conducted an online survey to gain insights on common disturbances in everyday life, and how individuals deal with them. Furthermore, we asked participants to rate the perceived utility of a smartphone app that would allow them to anonymously share their privacy preferences with others nearby, whether they would be interested in knowing about others' preferences, and the perceived utility of their phone automatically adapting to those preferences.

4.1 Recruitment and Participants

Participants were primarily recruited from the campus population at the University of Ulm, which corresponds to a relevant target group for our app. The survey was completed by 101 participants between 18 and 57 years old (M=23), with 65 male and 36 female. Participants were well educated (61% high school degree, 33% university degree) and almost all owned a smartphone (95%). Furthermore, most participants (98%) were German, thus, the results may reflect respective cultural norms and conventions.

4.2 Survey Results

4.2.1 *Common disturbances*

Figure 1 shows the reported frequencies of common disturbances, where they occur, and what activities they impact. For each item we ran a Mann-Whitney U test to evaluate gender-specific differences. While no significant differences could be found for the source of disturbances and the impacted activities, we found significant differences for some of the reported locations.

The majority of participants (87.5%) reported to feel frequently or sometimes disturbed by loud music, followed by others' phone calls (71.9%), ringing phones (66.7%) and nearby conversations (61.5%). The more distracting nature of phone calls in relation to face-to-face conversations has also been confirmed by previous research [14, 15]. Reasons for that are the missing pieces of a conversation which one tries to complete and the fact that people tend to speak louder in phone calls than in normal conversations [15]. Less common sources of disturbances were noise of devices, and being photographed or approached by others. Further disturbances mentioned by individual participants were loud typing, notifications during a date, and crying babies.

Regarding reported locations, disturbances occured primarily during public transport (79.2%) and at university (67%), which reflects characteristics of the sample population. Almost half of the participants also stated to be frequently or sometimes disturbed in restaurants, at work, public places, and in supermarkets or shops. Disturbances occurred less often at home or at the library. Other individually mentioned locations of frequent disturbances were train stations, waiting rooms, cinemas, and fitness centers. We found significant gender-specific differences for four locations. Women reported to be more frequently-disturbed at restaurants (U= 3612, p=.005), at libraries (U=3719, p=.011), in supermarkets/shops (U=3737, p=.013), and during public transport (U=3785, p=0.019).

The most named disturbed activities were studying (75%), working (57.3%), and reading (54.2%). Individual participants further mentioned dating, cooking, cleaning, and having sex as frequently disturbed activities.

Based on these results, we derived salient disturbance factors which allow users to specify privacy preferences for different situations. These factors and their use in PriPref Broadcaster will be discussed in Section 5.

4.2.2 *Reducing disturbances*

We further asked participants about their strategies for reducing physical disturbances, and about their attitude towards a smartphone application that would support them in such situations. The results are shown in Figure 2.

Roughly half of the participants stated to frequently or sometimes take counter-measures to reduce disturbances. However, only 27% stated to actively approach others who cause disturbances. Most participants (73%) rarely or never confronted disturbers as it makes them feel uncomfortable (68%). Of the 60 participants who stated to approach other persons, only 28% reported that it often led to the end of the disturbance. Most (63%) were only successful in stopping the disturbance in some situations and 8% reported to never have success in this regard. We further found a significant gender-specific difference in the reported frequency of approaching others and the success of approaching. Men

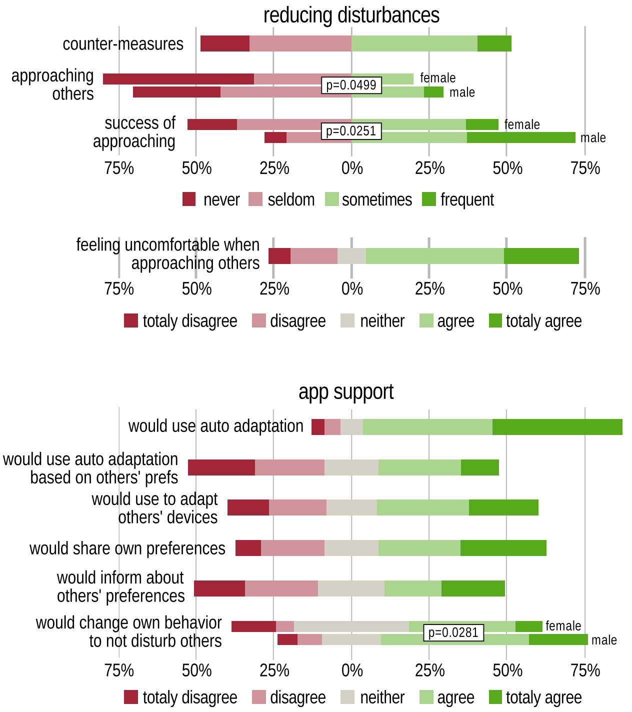


Figure 2: Frequency of strategies to reduce disturbances (*top*) and attitudes towards app features for supporting the reduction of disturbances (*bottom*).

approach disturbers more frequently (U=1373, p=0.05) and also reported to succeed more often in stopping a disturbance by approaching its source (U=549, p=0.025).

The reported experienced reactions of the persons approached varied from considerate or ashamed, to annoyed and violent. Negative reactions were primarily encountered in public transport. Therefore, instead of approaching disturbers, some participants reported to prefer changing their location if possible (5) (e.g., to a different seat on the train) or to isolate themselves from disturbances (6) (e.g., by listening to music with their headphones).

Regarding the support of reducing disturbances by a smartphone application, most participants (84%) would use it for the automatic adaptation of phone settings in order to reduce disturbances, but primarily based on own preferences. Only 39% stated they would allow automatic adaptation based on preferences received from persons nearby. On the other side, roughly half of the participants could imagine to use such an app to share their own privacy preferences (54%) and having devices of other persons adapt to their communicated preferences (52%). This shows that the acceptance for using the app for reducing disturbances by others is higher than for reducing one's own disturbance of others.

However, 38% could imagine to inform themselves about others' preferences – mostly in public places like public transport, restaurants, and waiting rooms. 58% also stated they would change their behavior in some situations, if such an app would inform them about others' preferences. Here we found that men were significantly more likely to potentially change their behavior than women (U=1384, p=0.028).

5. SIGNALING PRIVACY PREFERENCES

Based on the survey results, we defined a set of privacy preference dimensions and developed wireless broadcasting mechanisms to enable users to signal their individual privacy preferences in their physical proximity.

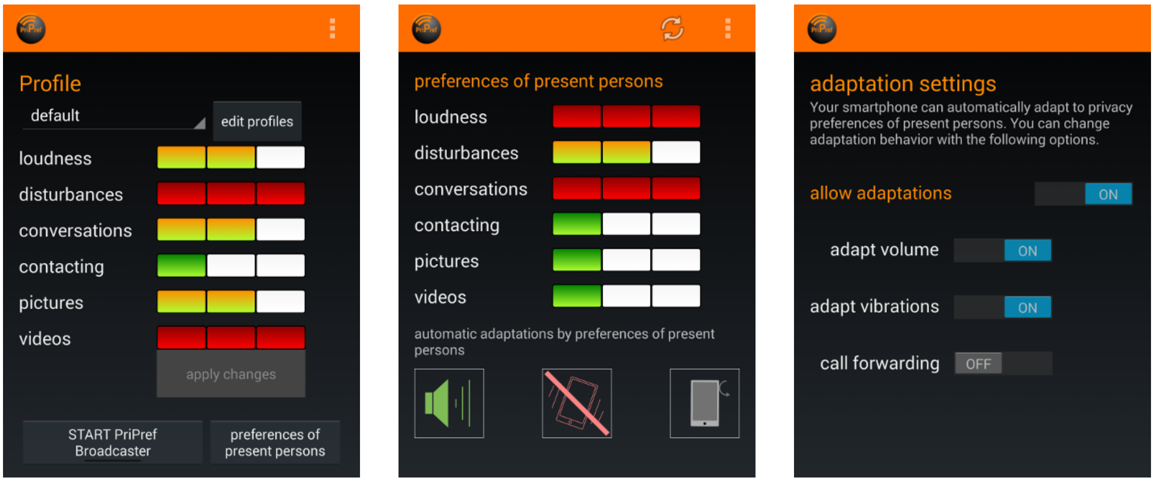
5.1 Salient Disturbance Factors

From the survey results and the common sources of everyday disturbances in particular (cf. Fig. 1), we derived six salient disturbance factors for which users can individually specify their preferences:

1. *Loudness:* Users can specify how accepting they are of loud noise/sounds nearby, or whether they prefer quiet. This factor concerns the general sound level in a user's environment. This includes loud music, which was the most frequently reported source of disturbance in our online survey.
2. *Disturbances:* Users can specify their acceptance of specific acoustic disturbances, e.g., ringing phones, noise from games or typing.
3. *Conversations:* Whether or not users approve of conversations between nearby persons and phone calls taking place in their vicinity.
4. *Contacting:* Whether users are open to being approached by others. While being approached was a less frequent source of disturbance in the online survey, we chose to include this factor in order to study its utility in real world situations.
5. *Pictures:* Whether users mind it when they are in other people's photos or when others take pictures of them. This factor concerns pictures being taken while the user is in the camera's field of view, regardless of whether this is intended or unintended by the person taking the picture.
6. *Videos:* This factor is the same as the *pictures* factor but pertains to video recording, including other persons as well as surveillance cameras. We included this as a separate dimension, because video recording can be considered more invasive than taking single pictures and hence should be reflected as a separate factor.

The user's level of acceptance of a given disturbance factor can be specified on a 3-point acceptance scale: *accept*, *tolerate*, and *reject* (see Fig. 3). *Accepting* a factor means that the user is open to it in the current situation, i.e., it is not perceived as a disturbance. For example, accepting loudness means that the user does not mind loud music or a loud environment in the current situation. *Tolerating* a factor means that the user would prefer a reduction of the disturbance but also accepts it in the current situation. Finally, if a factor is *rejected* the user has a strong preference against this factor. For example, a user might reject loudness during activities that require quiet, such as studying or working, which were the two most frequently reported disturbed activities.

To ease preference management, our signaling application enables users to specify preference profiles for recurring situations. For example, a user may create profiles related to activities such as *studying*, *working*, *relaxing*, or *reading*.



Profile

default | edit profiles

loudness	🟨🟨⬜
disturbances	🟥🟥🟥
conversations	🟨🟨⬜
contacting	🟩⬜⬜
pictures	🟨🟨⬜
videos	🟥🟥🟥

apply changes

START PriPref Broadcaster | preferences of present persons

preferences of present persons

loudness	🟥🟥🟥
disturbances	🟨🟨⬜
conversations	🟥🟥🟥
contacting	🟩⬜⬜
pictures	🟩⬜⬜
videos	🟩⬜⬜

automatic adaptations by preferences of present persons

adaptation settings

Your smartphone can automatically adapt to privacy preferences of present persons. You can change adaptation behavior with the following options.

allow adaptations: ON

adapt volume: ON

adapt vibrations: ON

call forwarding: OFF

Figure 3: PriPref Broadcaster: Main view to set privacy preferences (*left*), environment view to inform about others' preferences (*middle*), and adaptation settings view to configure automatic adaptations (*right*).

5.2 Preference Broadcasting

In order to effectively signal a user's privacy preferences to other persons nearby, we identified three basic requirements that must be met by potential broadcasting mechanisms:

- *Ad-hoc communication:* To allow fast and seamless communication of privacy preferences, a broadcasting mechanism should not rely on centralized solutions requiring Internet connectivity. Furthermore ad-hoc communication should work without requiring lengthy connection establishment between devices.
- *Proximity-based communication:* Privacy preferences only need to be signaled to other persons nearby (potential disturbers). In order to provide a meaningful overview (see Fig. 3) of the dominant privacy preferences in a receiver's current environment, broadcasting of privacy preferences should be limited to the range required for reaching those potential disturbers.
- *Existing technology:* Signaling mechanisms should be based on existing and widely available technology to facilitate fast adoption and increase the utility of signaling privacy preferences. Requiring special technology would unnecessarily limit the number of potential receivers of broadcasted preferences.

Based on these requirements, we developed two independent wireless broadcast mechanisms that leverage WiFi and Bluetooth, respectively. Both technologies are available on most smartphones and mobile devices and have a range of 10–100 meters, which covers the physical area around a user in which potential disturbers may be located. While both technologies typically require the establishment of a connection, we avoid connection establishment by embedding privacy preferences directly into WiFi beacon messages and Bluetooth device names, which can be received by other devices without the need of a connection. Similar approaches have been proposed to advertise data practices of smart devices [31, 30] and public display interaction [11]. However, we are the first to leverage this general approach to enable individual users to dynamically communicate their privacy preferences in physical proximity.

Supporting signaling over two technologies further has the advantage that our system can dynamically switch between them depending on which one is currently not in use for other purposes, e.g., using WiFi for preference signaling when Bluetooth is used for a headset connection.

We encode privacy preferences in a plain text string that starts with the prefix `pripref`, followed by the 6 disturbance factors in the order given in the previous section. For each disturbance factor, the user's acceptance is coded by a single digit: 1 (accept), 2 (tolerate), or 3 (reject). For example, the string `pripref:323123` encodes the preference: *reject loudness*, *tolerate disturbances*, *reject conversations*, *accept contacting*, *tolerate pictures*, and *reject videos*. Note that this encoding scheme is extensible. Further acceptance levels as well as disturbance factors could be added in the future.

5.2.1 *Preference signaling in WiFi beacons*

The IEEE 802.11 WiFi standard [21] employs so called beacons to announce available WiFi networks. Although rarely utilized, these beacons can be used to communicate custom information by either encoding it in the service set identifier (SSID) or optional information elements [10], while maintaining standard compliance. The SSID field typically contains user-friendly names of WiFi access points and is limited to 32 bytes. Information elements can be appended to beacons to carry additional information of up to 252 bytes. While using information elements is standard compliant, existing WiFi drivers need to be patched in order to support processing of custom information elements. Thus, we combined the use of SSID and information elements [30] in order to support non-patched, off-the-shelf devices.

5.2.2 *Preference signaling in Bluetooth device names*

Similar to the SSID method described above, Bluetooth device names can also be leveraged to broadcast custom information of up to 248 bytes [11]. The Bluetooth discovery process is more energy efficient than scanning for WiFi beacons, but takes significantly longer. Therefore, we propose to combine both methods and to primarily use WiFi unless the battery level is low or the device is currently using the WiFi connection to transmit or receive data.

Our current prototype implementation does not yet include integrity protection mechanisms to protect agains forged preference broadcasts. The anonymity of broadcasts further depends on the assumption that the Bluetooth or WiFi MAC address cannot be associated with a particular person. Both issues can likely be addressed by leveraging pseudonyms and digital signatures similar to proposals for ad-hoc car-2-car communications [39].

5.3 Dynamic Settings Adaptation

When privacy preferences are signaled with either approach outlined above, the preferences are received by devices of other persons in range and processed by our application. Accumulated received preferences can provide an overview of the prevalent preferences in the current environment. However, based on others' received preferences, our system can also automatically adapt device settings, such as the volume, vibration mode, and call forwarding settings. Whether adaptation is required is determined based on the first three disturbance factors, *loudness*, *disturbances*, and *conversations*. The other three disturbance factors are typically not influenced by the settings of a mobile device. However, if device settings would allow to block the camera and video function, this could pose another possible adaptation. We currently support three possible adaptation decisions, to demonstrate the potential of dynamic settings adaptation:

1. *Reduce volume and system sound:* Applied when the majority of persons in proximity prefers a quiet environment, that is more than 50% reject *loudness.*

2. *Mute and activate vibration mode:* Applied when the majority (>50%) rejects acoustic *disturbances.*

3. *Redirect incoming calls to mailbox:* Applied when *conversations* are rejected by the majority (>50%).

While adaptation decision 3 is independent of the other two decisions, decision 2 obviously outweighs decision 1. Thus, regarding acoustic noise of a mobile device, the *disturbance* factor is weighted higher than the *loudness* factor in our current adaptation mechanism. Further, tolerated factors are not respected in the adaptation mechanism but could support more nuanced adaptations in a future version. All three adaptations can be manually enabled or disabled by the user.

5.4 Android Application

We implemented the features described above in *PriPref Broadcaster*, which is a mobile application for Android. We created two versions of our system. Our fully functional prototype is based on a custom Android image in which we patched the WiFi device drivers in order to enable broadcasting and receiving WiFi beacons with information elements. We further created a public version[1] that only uses Bluetooth to broadcast preferences and, hence, can be readily installed and used on any unpatched Android phone.

Figure 3 gives an overview of the application. In the main view, users can set their preferences, create profiles, and start/stop the broadcasting of their preferences. The acceptance levels are represented with the traffic lights metaphor (green=accept, yellow=tolerate, red=reject). The second view provides an overview about the preferences of other persons present in the user's proximity. While the first version of the app used a pie chart visualization for this overview the usability study revealed that this approach was counter-intuitive. Thus the final version (shown in Fig. 3) uses the same traffic light visualization as in the settings view. To ensure that minorities with more restrictive preferences are properly visible, a factor is displayed red when at least some persons reject this factor, and the total number of persons rejecting and tolerating this factor exceed 50% together. In all other cases the displayed acceptance factor is averaged across all received broadcasts.

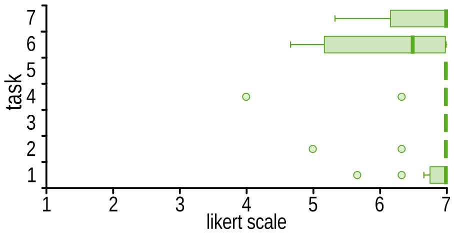


Figure 4: ASQ results for each of the seven usability tasks with ratings on a 7-point likert scale.

Three symbols at the bottom of the view further show whether and how the settings of the user's phone have been automatically adapted based on those received preferences, i.e., if the phone's volume has been changed, the vibration settings have been changed, or call forwarding has been activated. Finally, the adaptation settings view enables users to control whether phone settings should be automatically adapted at all, and to enable/disable automatic adaptation of volume, vibrations, and call forwarding.

6. EVALUATION

We first conducted a small-scale usability study with an initial prototype version. The results informed the design of the public version of our app, shown in Figure 3. This version was deployed on the personal smartphones of 28 participants and evaluated in a field trial of 5 days.

6.1 Usability Study

The usability study was conducted with 10 computer science students (2 female, 8 male; avg. age 25 years, SD=3). After a short introduction to the app, participants performed seven tasks that covered all app features: profile creation (t1), changing (t2) and deletion (t3); broadcast starting (t4) and stopping (t5); adaptation configuration (t6); and gaining an overview of others' preferences (t7). Participants completed the ASQ questionnaire [33] after each task, and the PSSUQ [33] at the end, followed by a short interview.

6.1.1 Results

Figures 4 and 5 show the positive feedback of participants for ASQ and PSSUQ, respectively. All tasks were rated as satisfactory (above neutral) in the ASQ. Only the configuration of adaptation (t6) and informing about others' preferences (t7) received slightly lower scores. The interviews revealed that adaptation configuration was rated lower, because the menu which included the entry to open the adaptation view was not available from all other views. Information

[1] The PriPref Broadcaster application is available in the Google Play store: `https://play.google.com/store/apps/details?id=com.pripref.app`

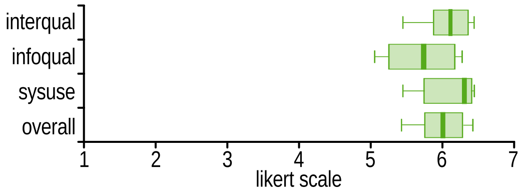


Figure 5: PSSUQ results for the application with ratings on a 7-point likert scale.

about others' preferences was rated lower due to a counter-intuitive pie chart visualization of others' preferences. Both issues have been addressed in the design of the public version of our application, shown in Figure 3.

The exit interviews further revealed that all of the ten participants saw utility in our application and found it easy to use. Nine participants stated that they would use the app in everyday situations and remarked on several situations in the past (e.g., at work or in public transport), in which the app would have been useful.

6.2 Field Trial

To investigate how PriPref Broadcaster would be used in everyday situations, we conducted a 5-day field trial with a deployment on devices of 28 participants, who were students and employees recruited from our campus population.

Participants were asked to adjust the app settings during their daily activities, whenever their actual privacy preferences changed. They were further asked to create profiles for recurring situations, if they thought it would be useful, and to start broadcasting when they wanted others to know about their preferences. Furthermore, they should configure adaptation settings as preferred. The app automatically reminded them to provide feedback on their usage every 5 hours. After using the app for 5 days, participants were asked to answer a post-study questionnaire and to provide demographic data. In addition, the application logged whenever broadcasting was started or stopped, adaptation settings changed, own preferences or received preferences of present persons changed, and when the user viewed others' preferences. As a reward, participants could enter into a lottery of 5 shopping coupons with a value of 10 to 50 Euros.

6.2.1 Participants

Participants consisted of 2 groups. Most of them (24) freely installed the app motivated by distributed flyers on our university campus. Those participants took part in the study anonymously by downloading the app from Google Play and using it at their discretion. Because we could not assure that those participants were in physical proximity of each other when using the app, we were primarily interested in how they would use the app for specifying privacy preferences. Of those 24 participants, 13 provided demographic data (all male, 10 students and 3 employees) and 15 provided explicit usage feedback. Furthermore, 10 persons used the app for the complete duration of 5 days, while others used the app only for 3 days (2), 2 days (5), and one day (8). We did not collect contact information of participants to respect their anonymity and could therefore not probe why they did not use the app for the complete duration.

We further recruited a group of 4 students (3 male, 1 female), who regularly spent time together in a shared lab space at our institute, in which they worked or studied. This group allowed us to gain a better indication of the effectiveness of our approach when all persons in physical proximity are using the application. All participants of this group used the app for the complete duration of 5 days and provided explicit usage feedback.

Overall, the 17 persons who provided demographic data were aged between 18 and 31 (M=25) and most (16) had a computer science background.

6.2.2 Results

Across all 28 participants who contributed data to our study, we logged 1,220 application events, of which 511 ($\overline{x}$=18, M=4, SD=27) were environmental changes (i.e., the received preferences of nearby persons changed), 247 profile changes by the user ($\overline{x}$=9, M=4, SD=11), 185 transmission starts to broadcast preferences ($\overline{x}$=7, M=3, SD=11), 177 views of environmental preferences ($\overline{x}$=5, M=3, SD=9), 83 transmission stops ($\overline{x}$=3, M=3, SD=9), and 17 changes of adaptation settings ($\overline{x}$=1, M=0, SD=1).

Situations of use.

The explicit usage feedback provided by participants indicates that the app was mostly used while studying (34%), relaxing (28%), or working (22%) which corresponds to the results of our online survey. In the field study, participants used the app mainly at home (40%), at work/university (37%), and in public transport (11%). In the online survey, "at work" was indeed a frequently mentioned location where disturbances occur often, while "at home" was the least frequently named location, and "public transport" the most frequently mentioned location of disturbances. The low number of uses in public transport might be due to the low prevalence of the app and thus lacking real effects of privacy preference broadcasts. In the post-study survey one participant stated *"I assumed that people do not have the app. So I wanted to save time and effort"*. The large number of uses at home might be caused by the fact that participants described that they used the app in 39% of all cases for testing purposes, i.e., to play around with our app. In 43% it was used to reduce disturbances, and in 18% to avoid disturbing others. Thus, participants preferred to reduce disturbances caused by others by signaling privacy preferences, but were less interested in informing themselves of others' preferences. While this reflects the results of our online survey (see Figure 2), the probing nature of the study, i.e., only few users have the app, made it unlikely for participants to receive preference broadcasts from other users in many situations, e.g., when not on campus.

In situations that prompted participants to change their privacy preferences, they categorized people around them as strangers in 42% of the cases, in 31% as friends, in 20% as colleagues, in 6% as family members, and in 16% of all cases participants were alone when using the application. This result might support our assumption that the app is especially useful to communicate privacy preferences in situations with strangers, as directly approaching those people to mitigate disturbances may be unpleasant or socially awkward.

Preferences and profiles.

In total, participants changed their preferences at 247 occasions. Figure 6 shows the distribution of configured preferences. While the first four disturbance factors (loudness,

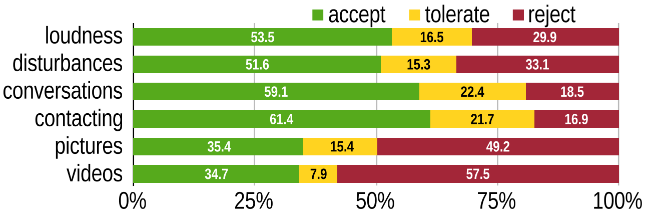
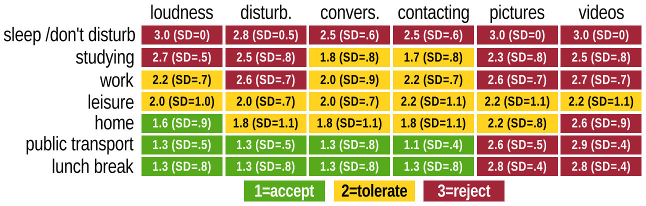


Figure 6: Preference distribution of all participants during the 5 day field trial.



	loudness	disturb.	convers.	contacting	pictures	videos
sleep /don't disturb	3.0 (SD=0)	2.8 (SD=0.5)	2.5 (SD=.6)	2.5 (SD=.6)	3.0 (SD=0)	3.0 (SD=0)
studying	2.7 (SD=.5)	2.5 (SD=.8)	1.8 (SD=.8)	1.7 (SD=.8)	2.3 (SD=.8)	2.5 (SD=.8)
work	2.2 (SD=.7)	2.6 (SD=.7)	2.0 (SD=.9)	2.2 (SD=.7)	2.6 (SD=.7)	2.7 (SD=.7)
leisure	2.0 (SD=1.0)	2.0 (SD=.7)	2.0 (SD=.7)	2.2 (SD=1.1)	2.2 (SD=1.1)	2.2 (SD=1.1)
home	1.6 (SD=.9)	1.8 (SD=1.1)	1.8 (SD=1.1)	1.8 (SD=1.1)	2.2 (SD=.8)	2.6 (SD=.9)
public transport	1.3 (SD=.5)	1.3 (SD=.5)	1.3 (SD=.8)	1.1 (SD=.4)	2.6 (SD=.5)	2.9 (SD=.4)
lunch break	1.3 (SD=.8)	1.3 (SD=.8)	1.3 (SD=.8)	1.3 (SD=.8)	2.8 (SD=.4)	2.8 (SD=.4)

1=accept 2=tolerate 3=reject

Figure 7: Common profiles created during the field trial and average acceptance of disturbance factors for each profile among participants.

disturbances, conversations, and contacting) were considered acceptable in more than 50% of all preference configurations, picture taking (49.2%) and video recording (57.5%) were mostly rejected. Conversations (18.5%) and contacting (16.9%) received the lowest rejection rate compared to loudness (29.9%) and disturbances (33.1%). The results show that taking pictures and videos are major privacy concerns in most situations and that conversations and being approached are perceived as less disturbing than loudness and acoustic disturbances.

Participants created 76 preference profiles in total ($\overline{x}$=3.4; SD=2.1), from which we identified 7 profile categories: *work* (n=9), *studying* (n=7), *public transport* (n=7), *lunch break* (n=6), *leisure* (n=5), *home* (n=5), and *sleep/do not disturb* (n=4). Figure 7 shows the average acceptance of the disturbance factors for each category. The most restrictive profile categories were *sleep/don't disturb*, *studying*, and *work*.

Automatic adaptation.

Four of the 28 participants enabled the automatic phone adaptation in 9 situations, mostly during studying and working (5). While volume adaptation was allowed in all cases, vibration adaptation was disabled once. Call forwarding was never allowed. The low acceptance of automatic adaptation was also confirmed in the post-study survey. Only 3 participants stated they would use the mechanism in everyday situations. One participant stated that he would never use automatic call forwarding and another stated that he switched off adaptation as he was afraid that his alarm would be muted as well. However, all would use the app to signal their own preferences, and 80% indicated that they would use it to learn about others' preferences.

Qualitative results.

The four students who actively used the app in their shared work space independently reported to like the opportunity of sharing their preferences with the others. They stated that the app increased their awareness and consideration of each others' preferences and in most situations reduced unwanted disturbances. However, in some situations they missed an option to more explicitly notify others about their preferences. One participant compensated the lack of explicit notifications by holding up his phone with the app displaying his preferences which resulted in the end of a disturbance. Related to this, two participants stated that they would like to receive notifications whenever preferences of present persons changed in order to adapt their behavior accordingly.

Another participant further stated that he would like to be able to add more details about a disturbance or some short messages to the preferences in order to specify what aspects are specifically disturbing, e.g., what kind of conversations. One participant would have liked to be able to share preferences with his real identity rather than anonymously, at least in some situations. For instance, to allow others to know who does not want to be contacted.

6.3 Limitations

A limitation of our evaluation is the sample size of 10 participants for the usability study and 28 participants for the field trial. As in the online survey, all participants were German which might influence results due to cultural norms. Especially the preferences and common profile categories could significantly differ among countries and cultures. Furthermore, only 14 participants participated for 5 full days in the field trial, while others used the app for fewer days. Due to the anonymous nature of the study, the reasons for not using the app longer remain unknown. One reason might be the low effectiveness of the approach when not many others use the app, an effect that is unavoidable in such a probing study. Nevertheless, the positive and homogeneous results of the usability study have also been confirmed during the field trial, which provided valuable insights on how preference signaling is used in everyday situations. Especially the collaborative usage of the app in a shared lab space by 4 participants provided interesting insights and showed the effectiveness of our approach. However, further studies are required to show the effectiveness in different environments and with larger groups.

7. DISCUSSION & FUTURE WORK

The results of our online survey revealed common sources of everyday disturbances, such as loud music, others' phone calls and conversations, or photo taking. Most participants felt uncomfortable approaching others causing such disturbances. Especially women reported to less often confront disturbers, and – if they do – having less success in ending the disturbance. PriPref Broadcaster provides an anonymous and easy to use approach to signal one's privacy preferences concerning undesired disturbances in such situations. Furthermore, it allows users to learn about others' preferences and to automatically adapt phone settings based on dominating preferences.

While the results of our evaluation studies are promising and indicate that the concept of privacy preference signaling was highly accepted, perceived as useful, and would be used in many everyday situations, the effectiveness has only be confirmed in a limited setting, and requires further evaluation with larger participant groups. A major factor that influences the effectiveness of our approach is the required prevalence among users. The motivation of sharing preferences depends on the assumption that others can be made

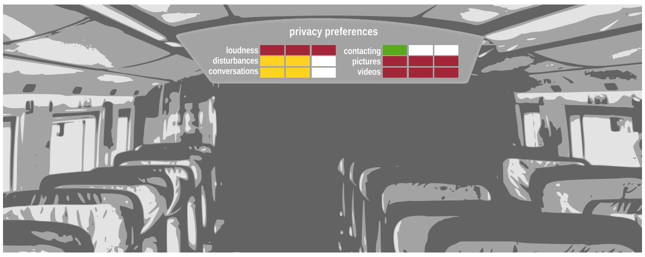


Figure 8: Sketch of a display in public transport which summarizes prevalent privacy preferences.

aware of one's preferences and change their behavior accordingly. While our results suggest that automatic adaptation of phone settings is less accepted, the online survey and field trial showed that people nevertheless are willing to inform themselves about others' preferences and indicate that they would adjust their behavior if required. To support this further, the overview screen of others' preferences (see Fig. 3) could display privacy notices that nudge users to adjust their behavior, or suggest adequate phone settings with respect to the current preferences.

Providing awareness of privacy preferences even without a large number of application deployments could be supported via proxy devices, e.g., through public displays which could visualize the combined preferences of persons nearby. For example, displays at study rooms or train compartments, as illustrated in Figure 8, could summarize dominant preferences of present persons signaling their preferences. Persons could then choose a seat on the train or in the study area that best matches their own preferences or adjust their behavior accordingly. While such displays would only be able to communicate preferences of persons using the application, it could also motivate others to obtain and use the application as well, in order to also signal their preferences. We are planning to investigate such proxy devices and their impact on users in future work.

Further, as suggested by several participants, we plan to investigate targeted just-in-time notifications about others' privacy preferences when a user starts an activity that would be against those preferences, e.g., when placing a phone call or opening the smartphone's camera application. Highlighting others' preferences in such situations could nudge people to behave more considerately with respect to those preferences (e.g., moving to a different train compartment to place a phone call or not taking any pictures with other persons in the background).

8. CONCLUSIONS

Disturbances frequently occur in everyday situations (e.g., at work or in public transport) and are often caused by present persons or their mobile devices, e.g., loud music or others' phone calls and conversations. The results of our online survey showed that most participants felt uncomfortable approaching other persons causing such disturbances.

In order to support users in reducing everyday disturbances, we proposed PriPref Broadcaster as an anonymous and easy to use approach to signal one's privacy preferences concerning undesired disturbances. To achieve this, preferences are communicated in a user's physical proximity leveraging WiFi beacons and Bluetooth device names. Our Android implementation can be readily used on existing smartphones. It allows users to learn about the preferences of others nearby and to automatically adapt phone settings based on dominating preferences.

Results from our evaluation studies indicate that the concept of privacy preference signaling was highly accepted and would be used in many everyday situations. However, the automatic adaptation of phone settings based on others' preferences was less accepted showing that users still prefer manual control, which indicates an opportunity for the design of privacy notices that nudge users to adjust their behavior.

While the effectiveness of our approach strongly depends on its prevalence, we plan to investigate the impact of public displays that visualize the combined preferences of nearby persons and thus potentially could increase the motivation to install and use the application.

9. REFERENCES

[1] I. Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Publishing Company, USA, 1975.

[2] D. Avrahami, D. Gergle, S. E. Hudson, and S. Kiesler. Improving the match between callers and receivers: A study on the effect of contextual information on cell phone interruptions. *Behaviour & Information Technology*, 26(3):247–259, 2007.

[3] J. P. Birnholtz, C. Gutwin, and K. Hawkey. Privacy in the open: how attention mediates awareness and privacy in open-plan offices. In *Proc. Intl. Conf. Supporting Group Work*, pages 51–60. ACM, 2007.

[4] S. Bok. *Secrets: On the Ethics of Concealment and Revelation.* Pantheon Books, 1982.

[5] M. Boyle and S. Greenberg. The language of privacy: Learning from video media space analysis and design. *ACM TOCHI*, 12(2):328–370, June 2005.

[6] M. Boyle, C. Neustaedter, and S. Greenberg. Privacy factors in video-based media spaces. In S. Harrision, editor, *Media Space 20 + Years of Mediated Life*, pages 97–122. Springer, 2009.

[7] P. Brey. The importance of privacy in the workplace. In S. O. Hansson and E. Palm, editors, *Privacy in the Workplace*, page 119. European Interuniversity Press, Brussels, 2005.

[8] M. Brill, S. T. Margulis, and E. Konar. *Using Office Design to Increase Productivity*, volume 1. Workplace Design and Productivity, 1984.

[9] A. Cammozzo. TagMeNot – opt-out for pictures taken in public, Aug. 2014. `http://tagmenot.info/` accessed: 2014-08-07.

[10] R. Chandra, J. Padhye, L. Ravindranath, and A. Wolman. Beacon-stuffing: Wi-fi without associations. In *Workshop on Mobile Computing Systems and Applications*, pages 53–57. IEEE, 2007.

[11] N. Davies, A. Friday, P. Newman, S. Rutlidge, and O. Storz. Using bluetooth device names to support interaction in smart environments. In *Proc. MobiSys '09*, pages 151–164. ACM, 2009.

[12] E. De Croon, J. Sluiter, P. P. Kuijer, and M. Frings-Dresen. The effect of office concepts on worker health and performance: a systematic review of the literature. *Ergonomics*, 48(2):119–134, 2005.

[13] S. Ding. Users' privacy preferences in open plan offices. *Facilities*, 26(9/10):401–417, July 2008.

[14] L. L. Emberson, G. Lupyan, M. H. Goldstein, and M. J. Spivey. Overheard cell-phone conversations when less speech is more distracting. *Psychological Science*, Sept. 2010.

[15] J. Forma and S. A. Kaplowitz. The perceived rudeness of public cell phone behaviour. *Behaviour & Information Technology*, 31(10):947–952, 2012.

[16] S. Grandhi and Q. Jones. Technology-mediated interruption management. *International Journal of Human-Computer Studies*, 68(5):288–306, May 2010.

[17] S. A. Grandhi, R. Schuler, and Q. G. Jones. Telling calls: Facilitating mobile phone conversation grounding and management. In *Proc. CHI '11*, pages 2153–2162. ACM, 2011.

[18] T. Heimann, L. Jaume-Palasi, M. Köbele, M. R. Ulbricht, F. Pallas, J. Schallaböck, M. Senges, and G. Süß. Offlinetags website, Aug. 2014. `http://www.offlinetags.net/en/` accessed: 2014-08-07.

[19] J. Ho and S. S. Intille. Using context-aware computing to reduce the perceived burden of interruptions from mobile devices. In *Proc. CHI '05*, pages 909–918. ACM, 2005.

[20] S. E. Hudson and I. Smith. Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems. In *Proc. CSCW '96*, pages 248–257. ACM, 1996.

[21] IEEE. 802.11 standard for LAN/MAN, 2012.

[22] IntelPR. Intel survey finds 'digital over-sharing' is leading mobile etiquette faux pas, May 2012. `http://newsroom.intel.com/community/intel_newsroom/blog/2012/05/08/intel-survey-finds-digital-over-sharing-is-leading-mobile-etiquette-faux-pas`.

[23] N. Kern, S. Antifakos, B. Schiele, and A. Schwaninger. A model for human interruptability: Experimental evaluation and automatic estimation from wearable sensors. In *Proc. ISWC '04*, pages 158–165. IEEE, 2004.

[24] A. Khalil and K. Connelly. Improving cell phone awareness by using calendar information. In M. Costabile and F. Paternò, editors, *Proc. of the Intl. Conference on Human-Computer Interaction*, volume 3585, pages 588–600. Springer, 2005.

[25] A. Khalil and K. Connelly. Context-aware telephony: Privacy preferences and sharing patterns. In *Proc. CSCW '06*, pages 469–478. ACM, 2006.

[26] J. Knittel, A. Sahami Shirazi, N. Henze, and A. Schmidt. Utilizing contextual information for mobile communication. In *CHI '13 Extended Abstracts*, pages 1371–1376. ACM, 2013.

[27] U. König and J. Schallaboeck. Privacy preferences for E-Mail messages. Internet-Draft "draft koenig privicons 04", IETF Network Working Group, 2012.

[28] B. Könings, D. Piendl, F. Schaub, and M. Weber. PrivacyJudge: effective privacy controls for online published information. In *Proc. PASSAT '11*, pages 935–941. IEEE, 2011.

[29] B. Könings and F. Schaub. Territorial privacy in ubiquitous computing. In *Proc. WONS '11*, pages 104–108. IEEE, 2011.

[30] B. Könings, F. Schaub, and M. Weber. PriFi beacons: Piggybacking privacy implications on WiFi beacons. In *UbiComp '13 Adjunct*, pages 83–86. ACM, 2013.

[31] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proc. UbiComp '02*, pages 237–245. Springer, 2002.

[32] C. Laroche, B. Rochon, S. Pelletier, and J. Sasseville. Shoji: Communicating privacy. In *CHi '12 Extended Abstracts*, pages 1285–1290. ACM, 2012.

[33] J. R. Lewis. IBM computer usability satisfaction questionnaires: Psychometric evaluation and instructions for use. *International Journal of Human-Computer Interaction*, 7(1):57–78, 1995.

[34] C. R. Long and J. R. Averill. Solitude: An exploration of benefits of being alone. *Journal for the Theory of Social Behaviour*, 33(1):21–44, Mar. 2003.

[35] S. Marti and C. Schmandt. Giving the caller the finger: Collaborative responsibility for cellphone interruptions. In *CHI '05 Extended Abstracts*, pages 1633–1636. ACM, 2005.

[36] J. Mayer and A. Narayanan. Do not track – universal web tracking opt out, 2014. `http://donottrack.us/`, accessed: March 2014.

[37] A. Monk, J. Carroll, S. Parker, and M. Blythe. Why are mobile phones annoying? *Behaviour & Information Technology*, 23(1):33–41, 2004.

[38] K. Nagel, C. D. Kidd, T. O'Connell, A. Dey, and G. D. Abowd. The family intercom: Developing a context-aware audio communication system. In *Proc. UbiComp '01*, pages 176–183. Springer, 2001.

[39] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11):100–109, 2008.

[40] F. Roesner, D. Molnar, A. Moshchuk, T. Kohno, and H. J. Wang. World-driven access control for continuous sensing. Technical Report MSR-TR-2014-67, Microsoft Research, 2014.

[41] J. I. Rosenbaum. Privacy on the internet: Whose information is it anyway. *Jurimetrics*, 38:565, 1998.

[42] S. Rosenthal, A. Dey, and M. Veloso. Using decision-theoretic experience sampling to build personalized mobile phone interruption models. In *Proc. Pervasive '11*, pages 170–187. Springer, 2011.

[43] R. E. Smith. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet.* Privacy Journal, 2000.

[44] S. D. Warren and L. D. Brandeis. Right to privacy. *Harvard Law Review*, 4:193–220, 1890.

[45] A. F. Westin. *Privacy and freedom.* New York: Atheneum, 1967.

[46] S. Zulkernain, P. Madiraju, S. I. Ahamed, and K. Stamm. A mobile intelligent interruption management system. *Journal of Universal Computer Science*, 16(15):2060–2080, 2010.