What's the Value of Your Privacy? Exploring Factors That Influence Privacy-sensitive Contributions to Participatory Sensing Applications

Delphine Christin, Christian Büchner, Niklas Leibecke
Secure Mobile Networking Lab
Technische Universität Darmstadt
Mornewegstr. 32, 64293 Darmstadt, Germany
Email: delphine.christin@cased.de

***Abstract*—Mobile sensing applications leverage sensors embedded in today's mobile phones to gather both user-centric and environmental data in unprecedented quantity and quality. The collection of sensor readings annotated with time and location information may however endanger users' privacy, as they may reveal their routines and habits. Our paper investigates different factors that may foster user contributions to these applications despite the related privacy threats. In particular, we analyze the impact of demographics, incentives, and gathering conditions on both the importance and value of privacy by means of a questionnaire-based user study with 200 anonymous participants. Our results show that young participants already sharing information online are more susceptible to contribute to participatory sensing applications initiated by academic institutions for a mean monthly reward of 50 euros.**

***Index Terms*—Mobile computing, Social factors, Technology social factors, Privacy.**

I. Introduction

With more than 6 billion mobile subscriptions worldwide [1], mobile phones are ubiquitous and their technological advances have lead to the emergence of millions of novel applications available in, e.g., the Google Play Store [2] or Apple's App Store [3]. The class of participatory sensing apps focuses on the collection of data about the users and their environment using sensors available in their mobile phones, such as accelerometers, cameras, and microphones. Example applications include monitoring diets [4], road and traffic conditions [5], and noise pollution [6]. While these applications can improve the life quality of millions of potential users, they simultaneously convert mobile phones into miniature spies and put the privacy of contributing users at stake [7]. For example, pictures can reveal social relationships and visited locations, while accelerometer data can be exploited to identify users' current activities. The spatiotemporal annotations of the sensor readings may further reveal users' routines and habits [8].

In order to protect user privacy, different technical solutions tailored to the requirements of participatory sensing applications have been proposed, e.g., in [9], [10], [11]. Most of these solutions, however, focus on technical aspects and do not include the participants in the loop. In this paper, we focus on human aspects and more particularly, we aim at better understanding users' behaviors when contributing data to participatory sensing applicationsconsidering the existing privacy threats. Our ultimate goal is to identify user groups especially susceptible to provide personal data to such applications in order to later develop novel tailored methods to increase their awareness about potential privacy threats. Within the scope of this paper, we hence explore multiple factors that may influence users to contribute privacy-sensitive data to participatory sensing and make the following contributions:

1) We analyze the design space of factors, which potentially influence the contributions of privacy-sensitive information to participatory sensing applications.
2) We explore the impact of the identified factors on the importance and the value of privacy by means of a questionnaire-based user study.
3) Based on the results of this study, we identify user characteristics and campaign conditions that contribute to the revelation of personal information to participatory sensing applications.

The remainder of this paper is structured as follows. In Section II, we introduce the field of participatory sensing applications with a focus on the associated privacy threats. We analyze the design space and outline factors susceptible to influence the users' behavior in terms of privacy in Section III. In Section IV, we present the modalities of our user study and discuss the obtained results. After summarizing existing work in Section V, we make concluding remarks in Section VI.

II. Participatory Sensing Applications

In this section, we provide an overview of the stakeholders and architecture of participatory sensing applications illustrated in Fig. 1 and highlight corresponding threats to privacy.

A. Stakeholders and Architecture

In participatory sensing applications, participants gather sensor readings using their mobile phones. Sensor readings include sound samples, pictures and videos, and acceleration [7]. The sensor readings are annotated with time and location information and then reported to an application server, which is run by the application administrators. The administrators

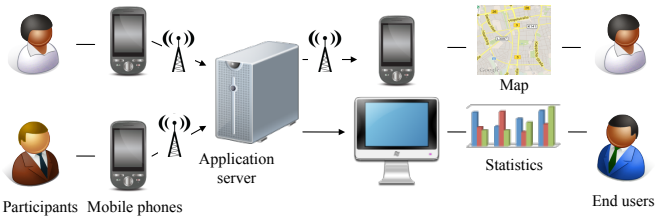

Fig. 1. Architectural overview of a typical participatory sensing application

thus have a direct access and control over the reported sensor readings. Eventually, the sensor readings are analyzed by either the administrators or third parties (e.g., doctors or scientists working in this field) depending on the application scenarios. The analyzed sensor readings are finally released in forms of maps or statistics to the end users including the participants themselves, their relatives, friends, or a larger public.

B. Threats to Privacy

The gathered sensor readings may reveal sensitive information about the participants to the involved stakeholders. In addition to the spatiotemporal annotations based on GPS, WiFi, or cellular network based triangulation, the locations visited by the participants can be inferred from, e.g., pictures or noise samples. This may leak privacy-sensitive information about the participants, such as their workplace and domicile locations as well as their routines and habits [8]. Additionally, frequent visits to hospitals may provide information about the users' medical conditions and attendance at political events may provide information about their political views [12].

But not only time and location measurements represent threats to privacy, automatically collected sound samples may also contain private conversations about intimate topics, while pictures and videos may give insights about the environment and social relations of the participants. Their release to unauthorized parties may lead to similar consequences as in online social networks where a woman lost benefits from her health insurance [13] and another her job [14] because of pictures published online.

Raw accelerometer readings may appear less threatening in revealing private information. However, information about the current participants' activity as well as their gait (and thus possible indications about their identities) may be inferred [15]. Text entries on mobile phones such as passwords may also be recognized solely based on accelerometer data [16].

In summary, the contribution of sensor readings to participatory sensing applications can severely compromise the privacy of the participants and may have severe consequences ranging from social to safety and security threats [8].

III. Design Space Analysis

Our ultimate objective is to provide guidelines to increase the awareness of potential users about the aforementioned privacy threats (cf. Section II). We thus analyze factors that may impact the willingness of participants to contribute data to participatory sensing applications. In particular, we investigate (1) demographic factors and their influence on the perceived importance of privacy and (2) contextual factors and incentive modalities. Our analysis builds upon existing work in orthogonal domains and serves as baseline for our user study presented in Section IV.

A. Demographics and Importance of Privacy

Among multiple demographical factors, we are first interested in the impact of the participants' *age* on their assessment of the importance of privacy in participatory sensing applications. Media often report that youths do not care about privacy especially in online social networks ([17], [18]). Also, their *relationships status* and the number of *children* may influence the participants' assessment, as these factors may increase the participants' need for intimacy [19]. Inspired from the results of [20], we further consider the influence of both *income* and *education achievements* on the importance of privacy. We extend the traditional demographics by adding the participants' *online sharing behavior* to the factors of interest. Participants already sharing a wealth of information online may consider their privacy protection as less important.

B. Incentive Modalities and Gathering Context

Different incentive modalities can be offered in participatory sensing applications, both in monetary and non-monetary form. In addition to the incentive nature, several factors can influence the corresponding participants' responsiveness. Again, the participants' *age* may influence their willingness to contribute personal data based on promised gains. We further believe that participants involved in *benevolent and altruistic activities* may be more prone to contribute due to the potential benefits for the community and request lower rewards. As shown in [21], the *nature of the party* deploying the participatory sensing applications as well as the *participants' relationships* to it may further alter the expressed privacy value. For example, it has been shown that users claim different rewards for scientific and corporate institutions [21]. The claimed reward may also depend on the *duration* of the data collection process. Similarly to the importance of privacy, online sharing behavior may influence the expected rewards, as users used to share personal information may do it for lower incentives.

IV. Questionnaire-based User Study

Next, we investigate whether the aforementioned factors have an influence on the expressed importance and corresponding value of privacy. To this end, we have initiated

an online questionnaire-based study. The questionnaire was available in both English and German and included 45 questions. The participants were recruited by announcements at our university. No incentives were offered for their contributions. 200 anonymous users contributed to our survey (24% female and 76% male). The participants were mostly German (89%) followed by Austrian (3%), while the remaining are distributed over several other nationalities. Their ages are between 18 and 58, with a mean age of 27. Additionally, 99% of our participants have at least one mobile phone and 67% would be ready to use it to contribute to participatory sensing applications. When asked for the reasons why they would not contribute to such applications, the most frequently given answer were their privacy concerns. The participants' mean rating about the importance of privacy is 5.82 on a scale from one (not important) to seven (very important). This confirms that privacy is globally an important concept for them. In what follows, we analyze and comment on the participants' answers.

A. Demographics and Importance of Privacy

In a first step, we focus on the six selected demographic factors and examine their influence on the importance of privacy expressed by the participants.

1) Age: We are first interested in verifying if the participants' rating about the importance of privacy increases with their age. An analysis of the correlation coefficient between both variables shows that they are only weakly correlated (r = 0.093). With a significance value p = 0.046 (< 0.05), the correlation is regarded as statistically significant on a 5% basis. In this case, the probability of having obtained this coefficient by chance is greater than five out of 100. A regression further shows that there is no linear relationship between the age and the expressed importance of privacy, but the result is not significant as p = 0.193. **Result**: Age and importance of privacy are correlated, but the linearity between both variables is not verified.

2) Education: Our second hypothesis is that the expressed importance of privacy increases with the education achievement(s). In our study, 81% of the participants completed secondary school, while 19% of have a university degree. Fields of study include business (52%), computer science (17%), engineering (10%), social sciences (7%), health care (4%) and others (27%) (multiple choices possible). A regression confirms our hypothesis, but the correlation between both variables is regarded as weak (r = 0.087). This implies that educational achievements play only a limited role in the rating of the importance of privacy. Both results are not statistically significant: p = 0.337 for the regression and p = 0.169 for the correlation. **Result**: The impact of the education achievements on the importance of privacy cannot be confirmed based on our study.

3) Income: We next consider the influence of the participants' income on their ratings. Among our participants, 62% participants have a monthly income between 0 and 1,000 euros, 14% between 1,001 and 2,000 euros, and the remaining between 2,001 and 3,000 euros. This distribution is principally due to the nature of our sample, mainly including students. Inspired from [20], we verify whether the importance of privacy also increase with increasing income in the case of participatory sensing applications. Both correlation and regression, however, show negative coefficients (-0.028 and -0.037, respectively). Higher income thus leads to a lower rating of the importance of privacy by our participants. Both significance values indicate that this hypothesis cannot be either confirmed or informed (p = 0.348 and p = 0.692, respectively). **Result**: The influence of participants' income on their rating is not statistically significant.

4) Relationship Status: We use an independent samples T-test to analyze the influence of the relationship status on the rated importance of privacy, since participants can be divided into two groups: singles and in a relationship. In our sample, 27% are currently in a relationship. By comparing the means, we observe that singles rate their privacy lower than participants in a relationship. A T-test, however, shows that the difference between both groups of participants is not statistically significant ($t(198)$ = 1.311, p = 0.422). **Result**: The influence of participants' relationship status on their expressed importance of privacy cannot be validated.

5) Children: Similarly to the relationship status, we test whether having children influences their rating, as 14% of our participants have children. **Result**: An independent samples T-test shows that having children does not lead to a significant increase in the importance of privacy ($t(198)$ = 0.197, p = 0.652).

6) Online Sharing Behavior: We finally analyzed if publishing more information online leads to a lower rating of the importance of privacy by the participants. For this analysis, we asked the 84% of participants registered in an online social network to indicate with whom (everybody, only friends, themselves, or not provided) they are sharing a set of 12 selected attributes (e.g., pictures, cell phone number, or date of birth). We attribute one point for each attribute shared with friends or everybody, and zero points otherwise. We then compute the sum over all attributes and compare it to the participant's rating. A regression shows a negative coefficient (B = -0.104) for the sum of published information in relation to the importance of privacy. Moreover, the obtained result is regarded as highly significant with a significance of 0.000. **Result**: There is a significant relationship between online sharing behavior and the importance of privacy expressed by the participants.

In summary, we have tested the influence of different factors of the importance of privacy expressed by our participants. While we have observed correlation between both factors and ratings, most of them are not statistically significant. This means that based on our sample of 200 users, no definite conclusions about the validity of our hypotheses can be drawn (neither in one way or the other). We could, however, confirm that ages and importance of privacy are correlated and the more the participants share information online, the lower they rate the importance of privacy.

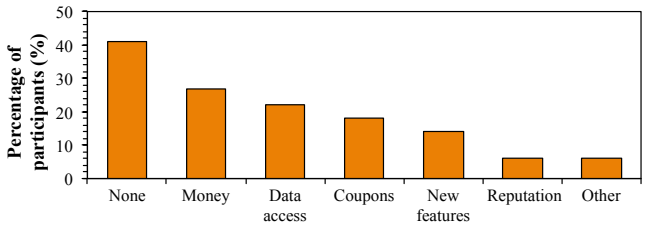

Fig. 2. Distribution of the participants' preferences in terms of incentives that would encourage their contributions to participatory sensing applications

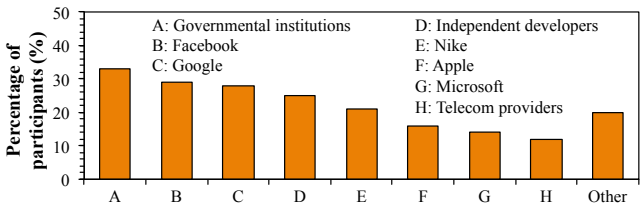

Fig. 3. Participants' evaluation of the trustworthiness of selected entities susceptible to organize participatory sensing applications

B. Incentives, Gathering Context, and Privacy Value

Next, we examine the impact of different factors on the value of privacy indicated by the participants of our study. To this end, the participants could select one or several incentives among monetary as well as non-monetary compensations, such as coupons, free access to additional functionalities or data, and increased reputation within the community. They could also select to contribute data without any compensation. As illustrated in Figure 2, 41% of our participants would contribute to participatory sensing applications for free, whereas 27% would claim a monetary reward, 22% would like to access additional data and 14% additional application features. 18% would be interested in getting coupons, while only 6% would be motivated by a higher reputation, e.g., stars, within the community. Furthermore, participants could indicate as free text, which monetary reward they would claim depending on different gathering scenarios. In what follows, we analyze their answers in correlation with the different factors introduced in Section III-B.

1) Age: We apply both a regression and a 1-way between-subjects *analysis of variance* (ANOVA). This test has the same purpose as a T-test, but allow us to analyze multiple groups of subjects. To be able to apply the ANOVA test, we cluster the participants into seven age groups having approximately the same size. While a regression shows a linear relationship between the age and the incentive values, the results of the ANOVA test indicate that the differences between the age groups are not statistically significant (p = 0.404). **Result**: The influence of participants' age cannot be confirmed on a statistical basis.

2) Volunteering and Altruism: Among our sample, 79 participants have already contributed to volunteering activities. Activities include being a sport trainer, helping in non-profit organization or youth work, volunteering at the church or at the voluntary fire fighter department. Moreover, 26% have an organ donor card and 29% have already donated blood, while 22% have already contributed to Wikipedia. Our hypothesis is that altruist or volunteering participants may contribute to participatory sensing applications for a lower reward than others. We have therefore asked which reward the participants would like to receive for a monthly contribution to a participatory sensing application. Our results show that the mean price indicated by the participants increases with the number of volunteering activities. However, a 1-way between-subjects ANOVA shows a significance of 0.942. **Result**: The difference between volunteering and non-volunteering participants is not significant enough to be generalized.

3) Online Location Sharing: We further assume that participants publishing their current location online may claim a lower reward than others. With a mean claimed monthly reward of 994 euros, the participants who already shared information claim lower rewards as compared to the remaining with a mean reward of 1,274 euros per month. We further analyze these results with an independent samples T-test, which shows equal variances but an insufficient significance with $t(198)$ = 0.692 and p = 0.490. **Result**: Sharing location information online does not significantly lead to lower expected rewards.

4) Academic vs. Corporate Institutions: In a first question, we selected several institutions, which may deploy participatory sensing applications and asked participants to indicate which one(s) they trust. As depicted in Fig. 3, more participants trust governmental institutions (33%) followed by Facebook (29%), Google (28%). Independent developers are rated as trustworthy by 25% of our participants, while Apple and Microsoft were chosen by 16% and 14% of the participants, respectively. Telecommunication providers show the lowest percentage with 12%. Asked if the size of the companies has an influence on their choice, 24% answered that they trust smaller companies and 21% larger ones. For 55%, the size of the companies does not influence their choice. Furthermore, we investigated the difference between the rewards claimed for either academic or corporate institutions for one month of data gathering. The results are illustrated in Fig. 4 and show that 28% of the participants would contribute to a campaign organized by academic institutions for free as compared to 1% for corporate institutions. For academic institutions, the median bid is 50 euros and 0 and 500 euros for the first and third quartiles, respectively. In comparison, only 17% of the participants would claim the same reward for corporate institutions, 4% would do it for a lower reward, 39% for a higher reward, and 40% would definitely not contribute. In this case, the median bid is 100 euros per month, while the first and third quartiles are 0 and 1,000 euros, respectively. Based on these descriptive results, we further analyze whether the assumption that participants claim a lower reward from academic institutions can be validated on an analytical basis. We use a paired samples T-test in order to compare both answers given by the same participants. With $t(120)$ = 5.771

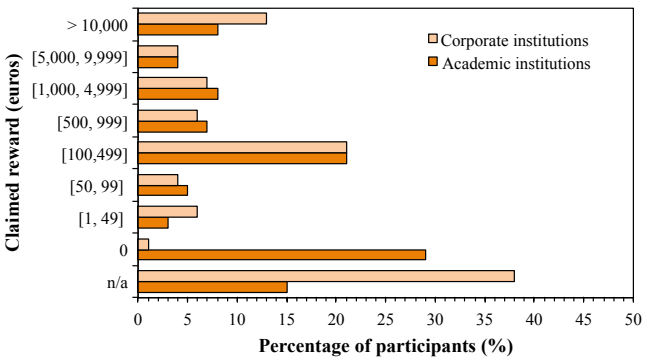

Fig. 4. Distribution of the monetary rewards claimed by the participants to contribute to a participatory sensing application initiated by either academic or corporate institutions during one month

and p = 0.000, the T-test confirms the statistical validity of our hypothesis. **Result**: Participants are ready to contribute to participatory sensing applications initiated by academic institutions for a lower reward as compared to corporate institutions.

5) Relationships with Academic Institutions: We next investigate whether past or current relationships with academic institutions influence the willingness of the participants to contribute to participatory sensing applications. An independent samples T-test confirms that existing relationships with institutions significantly influence the participants' decisions in contributing to such applications ($t(198)$ = 2.524 and p = 0.013). **Result**: Participants having a relationship with the entity initiating the participatory campaign are more willing to contribute to them.

6) Data Gathering Duration: We finally examine the impact of the data gathering duration on the reward claimed by the participants for one and 12 months, respectively. We would expect that the reward claimed for one year is twelve times the same for one month. However, it was demonstrated in [21] and [22] that participants tend to be more sensitive to the data collection purpose than its duration. This is confirmed in our sample, in which the mean reward claimed for a 12-month observation period is approximately 10 times higher than the mean reward claimed for a 1-month observation period. A paired samples T-test, however, shows that this difference cannot be generalized on a statistical basis ($t(46)$ = 1.712 and p = 0.094). **Result**: A longer gathering duration does not significantly mean a higher expected reward.

In summary, the descriptive analysis of the participants' answers allows us to identify several factors that influence their privacy value. However, only few of them could be confirmed by a statistical analysis. In particular, we have verified that participants claim lower incentives when academic institutions organized the campaigns as compared to corporate ones. The incentive values further decreases, when the participants have a relationship with these institutions. In average, participants are ready to provide their data for 50 euros to academic institutions, whereas they would request 500 euros from corporate institutions.

C. Study Summary

According to the results of our study, we can conclude that young participants sharing a wealth of information online are more likely to contribute to participatory sensing campaigns organized by academic intuitions. The willingness to contribute to these applications further increases, when the participants have a relationship with the organizing institutions. For 50 euros in average, the organizers could have access to their personal data gathered during one month. Participants are more reluctant to contribute to campaigns organized by corporate institutions and also claim a higher reward. By identifying these factors, we have refined the profile of participants susceptible to contribute privacy-sensitive data to participatory sensing applications. In the future, we plan to leverage this profile to develop mechanisms tailored to this user population in order to increase their awareness about potential privacy threats.

V. Related Work

While different user studies have been conducted on the topic of privacy in general or location privacy, they do not focus on participatory sensing applications as compared to our contributions. For example, the divergence between real and digital users' behaviors in terms of privacy is investigated in [23], while the rationality of users' privacy decisions is analyzed in [20]. Concerning location privacy, Brush et al. analyzed users' privacy concerns and the application of location obfuscation schemes, i.e., how users understood them and how they affect their behaviors, during a two-month location tracking period in [22]. Also using a questionnaire, Tsai et al. examined in [24] users' concerns about location tracking and the tradeoff between usefulness and risks of location-sharing technologies. Our work shares most similarities with the study conducted in [21]. Instead of only focusing on location privacy, we extend its scope to additional sensing modalities.

Additionally, user studies on incentive modalities and motivation factors have been conducted in orthogonal domains. For example, the motivations of contributors to surveys and Wikipedia are analyzed in [25] and [26], respectively. The responsiveness of survey participants to different incentive modalities is investigated [27]. Several incentive schemes tailored to the requirements of participatory sensing applications have also been proposed in [28], [29], and [30]. Their evaluations are however dominated by technical aspects.

As a result, we are the first to the best of our knowledge to investigate both privacy value and importance in the domain of participatory sensing applications based on a user study.

VI. Conclusions

Within the scope of this paper, we have identified and analyzed factors that can influence both the importance and value of privacy expressed by potential users of participatory sensing applications. For this analysis, we have conducted a

questionnaire-based study with 200 anonymous participants. While several trends have been identified using descriptive statistics, the following factors have been confirmed on a statistical basis: (1) young participants rate the importance of their privacy in participatory sensing applications lower than older people, (2) participants that already share information online rate their privacy as less important than others, (3) participants are more willing to contribute to campaigns organized by academic institutions than corporate ones, and (4) former and current students are ready to contribute to academic campaigns for a cheaper price than others. Consequently, such user population is potentially more exposed to contribute privacy-sensitive data to participatory sensing applications when the gathering conditions and incentives match those identified in this paper. Based on these results, we plan to conduct an additional user study with a larger number of participants and different backgrounds by using, e.g., Amazon Mechanical Turk in order to further explore the statistically unconfirmed trends.

ACKNOWLEDGMENT

This work was supported by CASED (www.cased.de).

REFERENCES

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

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

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

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

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

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

[7] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A Survey on Privacy in Mobile Participatory Sensing Applications," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1928–1946, 2011.

[8] K. Shilton, "Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection," *Communications of the ACM*, vol. 52, no. 11, pp. 48–53, 2009.

[9] R. K. Ganti, N. Pham, Y. Tsai, and T. F. Abdelzaher, "PoolView: Stream Privacy for Grassroots Participatory Sensing," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2008, pp. 281–294.

[10] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. 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.

[11] ——, "IncogniSense: An Anonymity-preserving Reputation Framework for Participatory Sensing Applications," *Pervasive and Mobile Computing*, vol. 9, no. 3, pp. 353–371, 2013.

[12] L. Liu, "From Data Privacy to Location Privacy: Models and Algorithms," in *Proceedings of the 33rd International Conference on Very Large Data Bases (VLBD)*, 2007, pp. 1429–1430.

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

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

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

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

[17] E. Nussbaum, "Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll," Online: http://nymag.com (accessed in 05.2013), 2007.

[18] J. Kornblum, "Online Privacy? For Young People, that's Old-School," Online: http://www.usatoday.com (accessed in 05.2013), 2007.

[19] S. T. Margulis, "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues*, vol. 59, no. 2, pp. 411–429, 2003.

[20] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy*, pp. 24–30, 2005.

[21] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A Study on The Value of Location Privacy," in *Proceedings of the 5th Workshop on Privacy in the Electronic Society (WPES)*, 2006.

[22] A. B. Brush, J. Krumm, and J. Scott, "Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (UbiComp)*, 2010, pp. 95–104.

[23] A. Shostack, "People Won't Pay For Privacy," in *Proceedings of the 2nd Annual Workshop 'Economics and Information Security'*, 2003.

[24] J. Y. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, "Location-Sharing Technologies: Privacy Risks and Controls," in *Telecommunications Policy Research Conference*, 2009, pp. 1–26.

[25] E. Singer, "The Use of Incentives to Reduce Nonresponse in Household Surveys," *Survey Nonresponse*, pp. 163–77, 2002.

[26] A. Forte and A. Bruckman, "Why do People Write for Wikipedia? Incentives to Contribute to Open-content Publishing," in *Proceedings of the Workshop on Sustaining Community: The role and Design of Incentive Mechanisms in Online Systems*, 2005, pp. 1–6.

[27] E. Ryu, M. P. Couper, and R. W. Marans, "Survey Incentives: Cash vs. in-kind; Face-to-Face vs. Mail; Response Rate vs. Nonresponse-Error," *International Journal of Public Opinion Research*, vol. 18, no. 1, pp. 89–106, 2005.

[28] J.-S. Lee and B. Hoh, "Sell Your Experiences: A Market Mechanism based Incentive for Participatory Sensing," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2010, pp. 60–68.

[29] S. Reddy, D. Estrin, M. Hansen, and M. Srivastava, "Examining Micro-Payments for Participatory Sensing Data Collections," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (UbiComp)*, 2010, pp. 33–36.

[30] A. Albers, I. Krontiris, N. Sonehara, and I. Echizen, "Coupons as Monetary Incentives in Participatory Sensing," in *Collaborative, Trusted and Privacy-Aware e/m-Services*, ser. IFIP Advances in Information and Communication Technology, 2013, vol. 399, pp. 226–237.