Understanding the Valuation of Location Privacy:
a Crowdsourcing-Based Approach

Maija Poikela
Technische Universität Berlin
maija.poikela@qu.tu-berlin.de

Eran Toch
Tel Aviv University
erant@post.tau.ac.il

Abstract

The exchange of private information for services or other benefits is a commonplace practice today in the advent of mobile technology. In the case of mobile services, the exchanged commodity is increasingly often spatial location of the user. To decide whether this transaction is beneficial, the user needs to evaluate the exchange value of this commodity. To assess the value users give to their location, and to understand its relationship with location sharing, we conducted a study on a mobile crowdsourcing platform (N=190). We find that users' valuation of location privacy is dependent on the sharing scenario. For instance, when the location is to be shared with an untrusted advertiser, the users require a premium as compensation for their information. Additionally, benefit perception and trust are found to be connected with more frequent location sharing, while perceived risks and privacy concern are associated with sharing one's location less frequently.

1. Introduction

People's location information is increasingly considered a commodity. Using location-based services (LBS), location is constantly being collected by multiple parties: service providers collect the data for the offered services, but also for selling it to third parties. These use it for behavioral advertising based on our location or movement patterns. We can either protect our privacy by switching the location services off or by refraining from using these services, or accept the deal and decide that the benefit from sharing the location is worth the price of diminished privacy.

Users have various concerns when using LBS, including being stalked and revealing home location [1]. Also too well targeted adverts can create privacy concern [2]. The concerns can create anxiety, in particular if the user feels powerlessness and not in control [3]. This can also lead to decreased disclosure,

or restrict adoption of the service [2]. On the other hand, several benefits are available for the users of these services: finding restaurants or friends nearby, or informing others about one's whereabouts [4]. To assess whether or not the received benefit is worth the expected privacy risks, the user needs to perform a risk-benefit analysis [5], evaluating how much they value each side of the deal. Thus, using the service can be considered a privacy transaction.

The theory of planned behaviour [6] states that the intention to act is mediated by several attitudes towards the behaviour. First, the positive and negative outcomes are weighed – this corresponds to evaluating the benefits and risks of using LBS. Second, the subjective norms, being the social expectations around the behaviour, are evaluated. Third, the subjective and actual control over the action have their effect on intention, and on the behaviour. In this work, we assessed the influence of the risks and benefits, as well as that of the normative beliefs, on valuation of location privacy.

We studied how users of a crowdsourcing platform value their location privacy in several one-time sharing scenarios. We find that the amount of money offered for sharing a location, as well as the scenario of what is done with the data, have an influence on the willingness to share location. The sharing rates were altogether rather high, and the amount paid seemed to have an influence mostly in the scenarios where the location would be shared also with advertisers. In a scenario where the location would be shared with an untrusted advertiser, the sharing rate was significantly lower than otherwise. Normative beliefs did not turn out to be a significant factor in predicting location sharing behaviour. Rather than stating a specific monetary value that is needed in each situation for the location to be shared, we use the location valuation as an attempt to quantify privacy concern, and for evaluating the differences in location sharing patterns. The values per se vary largely from one country to another [7], and quite likely also from one city to another within a country, thus making results regarding the exact value less meaningful.

HICSS

2. Related work

During the last decade, geographical information is increasingly often combined with demographic information, and used for targeted advertising based on the users' geographical location. Crampton [8] states that this commodification of users' spatial information has led to the users being more easily monitored and their behaviour controlled, and might even encourage a surveillance society, creating a serious threat to individuals' data privacy. Nissenbaum proposed a concept of privacy as contextual integrity for evaluating the flow of information from individuals [9]. Based on a context and norms, an individual has certain expectations of what happens to information about one's person – whether or not such information is being collected, and who might have access to it. Collecting personal information might happen without the users' knowledge and consent, and with analysis and aggregation of information being easier than ever, the individuals' expectations of data privacy might not be met. The user might engage in an interaction in which they trade their privacy to a benefit, but unless the individual is fully aware of the terms of the interaction, their contextual integrity is jeopardized. Leszczynski describes *anxiety of control* related with geographical information of ourselves – the users have a desire to control the collection and use of this data, but feel powerlessness over the inability to do so [10].

Culnan and Armstrong [11] propose that *privacy calculus* takes place each time prior to the disclosure of personal information, within which the benefits of the transaction are assessed against the expected privacy risk. Also Dinev and Hart [12] present the decision to disclose personal information as a fully rational choice in the presence of privacy concerns. Preibusch however states that privacy concern does not necessarily lead to corresponding behaviour [13], but disclosure might be the best choice for a user in a given situation. Several works describe privacy concern and behaviour being at odds; a *privacy paradox* (e.g. [14]).

Various studies have assessed how much value users give to their privacy. Users have been found to sometimes give out personal data even for no compensation [15] – Rose reports that the users receive significant benefits from information exchange and thus the benefits outweigh the possible negative consequences. However, according to Tsai et al. [16], when presented with an option offering more privacy protection, users are willing to even pay a small premium for enhanced privacy.

In a study by Acquisti et al. [17], the order in which the user is offered a price for sharing private information influences the price that the user assigns to that piece of information. Other studies have found the willingness to divulge private information to be context-dependent; according to John et al., the users are more likely to disclose personal information in a very informal setting [18]. The users are on the other hand found to be poor decision-makers when assessing the privacy tradeoff, and likely to undermine long-term privacy risks for short-term benefits [19].

The users of LBS give varying privacy sensitivity ratings to different locations. In a study by Toch et al., the users shared location in a social setting with acquaintances [20]. Also, users were found to be more willing to share locations that have a large and diverge set of visitors. How much monetary value users give to their location privacy has been studied by Danezis et al. [21], where users gave hypothetical values for participating in a location-sharing study during a period of 28 days. The highest value for a location information was given by the users with most variance in their moving patterns [21]. Barak et al. found that location valuation is dependent on the type of location in sharing in a social context [22]. In a study by Cvrcek et al. [7], European university students were asked in an online questionnaire how much they would need to be compensated to participate in a month-long field study, supposedly with the location being tracked during this time. Later, they were told that also a commercial entity would be interested in the data. The study did not confirm the results by Danezis et al. [21] regarding the movement patterns. Also, in a study by Bernheim et al. [23] imitating the survey by Cvrcek et al. [7], the expected payment to participate in the study approximately doubled compared to the original findings, further suggesting that finding an absolute value for location privacy might not be the most useful and applicable result from such research.

Trust in the receiving entity has been found to decrease privacy concerns [24]. Also, service providers' attempts to enhance privacy might increase consumers' trust beliefs and thus mitigate privacy concern [25]. Furthermore, trusting beliefs might, in addition to mitigating concerns of privacy risks, increase the users' willingness to disclose information through LBS [25]. Finally, even though there is evidence of the users' initial concern becoming alleviated after a short period of time [26], according to Xu et al., privacy concern can hinder the use through inhibiting the adoption altogether [27].

3. Research method

To study valuation of location privacy in a one-time sharing situation, we conducted a study using a mobile crowdsourcing platform Crowdee [28]. While it is likely that the real-life user of LBS does not have a full control of the integrity of their data flows [29] and thus

cannot make a sound and fully informed value calculation, we make a simplification to concentrate on the accepted payment based on four different scenarios, leaving the assessment of knowledge and control to further studies. The users of the platform could take part in a task that had a base payment of 0.10 €, with a possible bonus mentioned. The size of the bonus was stated within the job, before the user could choose whether they wanted to share their location in that scenario or not. No other questions or tasks were involved so as to ensure that the bonus was indeed related with the location sharing task. Instead, merely opening the job, going through the description of the task and the location sharing task itself would grant the basic payment, irrespective of whether or not the participant decided to share their location.

The study was conducted in Germany, and the prerequisite for taking part was fluency in German; the crowd workers had taken a language test to proof eligibility. The participants, after having taken the task, were presented randomly one of the following four scenarios, which assessed the effect of different recipients and subsequent data use on the willingness to disclose location:

1. _Trusted Advertiser_: Sharing location with third parties, "for customer behaviour analytics purposes by a third party". A fake advert by a _trusted_ advertiser was shown within the task.
2. _Untrusted Advertiser_: Sharing location with third parties, "for customer behaviour analytics purposes by a third party". A fake advert by an _untrusted_ advertiser was shown within the task.
3. _Crowdee_: Sharing location with the crowdsourcing platform Crowdee, with an explanation given, that the data is used "For customer behaviour analytics purposes".
4. _Crowdee Users_: Sharing in a social situation with other crowd workers. Simulated profile cards of other crowd workers were shown on the map within the task.

For an untrusted advertiser, we chose a company that ranked in the bottom five out of the 127 companies analyzed in a study assessing the impact that German and international companies have on general wellbeing [30]. As an advertiser of high trustworthiness, we chose an organization ranking in the top five within the same study. Both of these chosen advertisers can be considered rather well known in Germany and familiarity could be assumed. The adverts had a link to the respective companies' web sites. The companies were not informed about the study nor were they involved in it in any way. Whether or not the participants believed that the adverts were genuine was
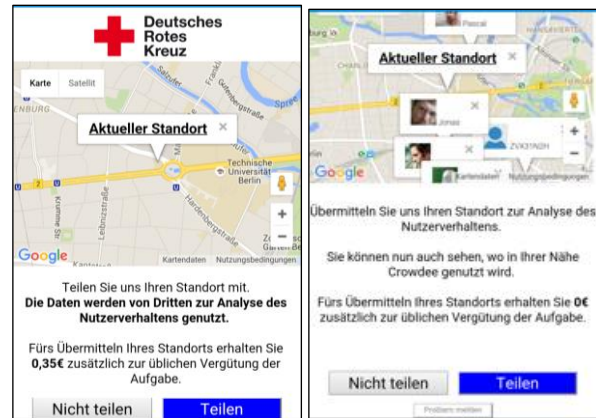

Figure 1: Screenshot of the location sharing task with a _trusted advertiser_, and of a scenario with _Crowdee users_. Before sharing the location, which was also shown on a map, the user could see the additional bonus that would be given for sharing. Not sharing would lead to a compensation of only the base payment of 0.10€.

not confirmed within the experiment, neither was it assessed whether or not the participants thought their location information would actually get in the possession of these advertisers. The scenarios were created as a web view that was integrated in the crowdsourcing platform, and the interaction flow between the app and the web view was seamless (cf. Figure 1 for a screenshot of the sharing situation with a trusted advertiser, and of that in a social situation).

To share one's location in any of the scenarios, the participant would select "Share" within the web view, in which case a bonus was paid in addition to the base payment of 0.10€. The amount of bonus was randomized between 0€ and 0.50€. A uniform distribution of payments with increments of 0.01€ was distributed between the tasks. In the case of the participant selecting "Do not share" within the web view, or leaving the web view without selecting either to share or not to share, only the base payment would be paid. As in real-life situations, the participants were not told about the possible subsequent data use or repurposing by third parties beyond the short explanation (e.g. "For customer behaviour analytics purposes").

Each eligible worker could take the task up to 10 times. A buffer time of two hours was enforced between tasks to avoid the task being taken several times in the same location. Order effects are not expected to influence the results because the payments are randomized every time the user participates in the task. The effect of the physical location in which the task was taken is out of the scope of this research.

4. Measures

All the questions in the used scales are presented in the Appendix.

Risk perception ($M = 4.57$, $SD = .95$; 9 items, Cronbach's α = .834) is measured using a scale under development, intending to measure the extent of risk perception on LBS. The questions are mainly based on previous research on which risks

the users are concerned about in this context [1]. The responses for this scale, as well as for *benefit perception, normative beliefs,* and *privacy concern* were measured on a fully labelled 7-point answer scale from *Fully agree* (6) to *Fully disagree* (0).

Benefit perception ($M = 4.80$, $SD = .97$; 6 items, Cronbach's α = .907) includes general statements regarding the benefits offered by LBS.

Normative Beliefs ($M = 3.46$, $SD = .96$; 3 items, Cronbach's α = .745) assess the extent to which the user believe that their peers have expectations regarding their behaviour, in this case using LBS.

Privacy concern ($M = 4.31$, $SD = .87$; 6 items, Cronbach's alpha = .719). The scale as reported by Morton [31] measures the user's inclination to protect their personal privacy and minimize the disclosure of personal information, or their *desire for privacy*. A fully labelled 7-point response scale was used.

Overall trust ($M = 3.94$, $SD = .82$; 16 items, Cronbach's α = .857) includes a combination of all of the 4-item measures of the level of trust the user has towards each of the instances the location is to be shared with (cf. Table 1). We expect this to give an indication of how trusting the user is in general.

5. Results

In total 1064 tasks were taken, out of which 72 were not carried out completely, meaning that the participant did not choose to either share or not to share their location. In 58 cases of these 72, there was a problem with the location setting of the phone and thus the map did not load, and as a consequence we disregard these cases from analysis; the remaining 14 cases are handled as "not shared". Additionally, all records from participants who were found cheating in

Table 1. Trustworthiness of the instances the location is to be shared with in the different scenarios was measured on a four-item scale.

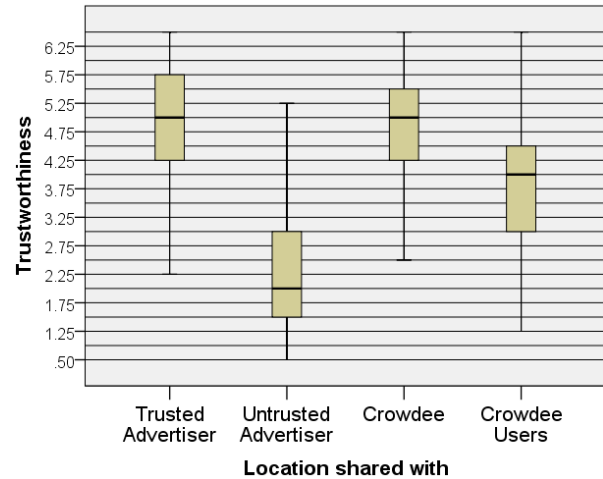|	Trusted Advertiser	Untrusted Advertiser	Crowdee	Crowdee Users
M	4.94	2.18	4.77	3.87
SD	1.03	1.10	1.00	1.07
Cronbach's alpha	.781	.768	.734	.750

Figure 2. Statistically significant differences were found in the trustworthiness of the different instances the participants would share their location with.

the follow-up study were disregarded, as well as those showing no variance in acceptance of the location sharing task, when at least two tasks were taken. The analysis in the following section is done based on the remaining 435 tasks that were carried out. Out of these, in 84% of the cases, the location was shared.

5.1. Demographics

190 unique crowd workers participated in the task, which could be repeated up to ten times. Altogether 109 crowd workers participated in the first follow-up questionnaire including the demographic questions and 16 questions about trustworthiness of the four recipients of location data; 105 responses were accepted based on the used trapping questions. 116 participated in the follow-up questionnaire regarding risks, benefits and privacy concerns when using location-based applications. Out of these, 107 were accepted based on the trapping questions. The 13 disqualified participants were left out of all the further analysis.The crowd was mainly young adults ($M = 28.76$, $SD = 8.83$). 60% of the participants were male. 33% had a university degree, and 46% were students. 35% of the participants stated that they are either currently or in the past practicing in the IT field.

5.2. Trustworthiness

We confirmed our expectations that the organization that we had chosen as a trusted advertiser was trusted significantly more than the one chosen as an untrusted advertiser. Also, Crowdee users were trusted more than the untrusted advertiser, but less than
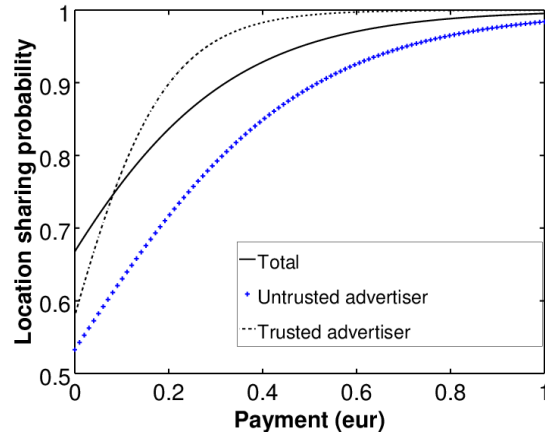
Figure 3. Logistic regression of acceptance of a location sharing task as a function of payment in Euro, giving a probability that a location is shared.

Crowdee or the trusted advertiser. The difference in trustworthiness between Crowdee and the trusted advertiser turned out not to be statistically significant; otherwise the trustworthiness scores differ from one another significantly ($F(3, 424)$, = 162.46, $p < .001$, cf. Figure 2). *Overall trust* is found to have a strong negative correlation with privacy concern ($r_s = -.55$, $p < .001$), suggesting that users who are generally trusting towards organizations have also less privacy concern.

5.3. Location sharing

We consider the binary location sharing task acceptance data per level of the amount paid for the task. A statistically significant effect was found for the sharing, with payment being higher in the cases when location was shared ($t(433) = -4.87$, $p < .001$). We also

Table 2. Parameters for a logistic regression model (cf. Eq. 1) for the location sharing scenarios with trusted and untrusted advertiser, as well as for the whole data set. The model fit in each case is also listed. The variables are payment (x_1) and trust (x_2).

	Trusted Advertiser	Untrusted Advertiser	Total
θ_1	9.598, $p = .003$	3.88, $p = .026$	30.82, $p < .021$
θ_2	.477, $p = .146$	.534, $p = .018$	1.193, $p = .025$
b	-1.967	-1.023	-5.031
R^2	.27	.15	.45

find that the scenario has a significant impact on sharing location ($X^2(3) = 15.22$, $p = .002$). *Risk perception*, as well as *privacy concern*, were found to be connected with sharing a location less frequently, and *benefit perception* as well as the *overall trust* were found to be connected with more frequent location disclosure; $t(52) = 2.54$, $p = .014$ (*risk perception*), $t(52) = 2.193$, $p = .033$ (*privacy concern*), $t(52) = -2.31$, $p = .025$ (*benefit perception*), $t(52) = -2.05$, $p = .046$ (*overall trust*). No effect was found with *normative beliefs*.

5.3.1. Logistic regression. The probability with which a user shares their location was modeled as a logistic regression, given by:

$$P(sharing \mid x) = \frac{1}{1+e^{-(\theta \cdot x + b)}} , \qquad (1)$$

where $x = (x_1, x_2, ..., x_n)^t$ are the constituent variables, and $\theta = (\theta_1, \theta_2, ..., \theta_n)$ and b the corresponding model parameters.

This was applied to the labeled dataset, estimating the two-class problem of whether or not the location sharing task is accepted as a function of *payment* (x_1). For the above single-variable model, we obtained $\theta_1 = .698$ and $b = 4.664$ (cf. Figure 3). This model however explains less than ten percent of the variance in sharing behaviour (*Nagelkerke R^2* = .09).

In order to enhance the model, we now consider also the effect of risks and benefits. This gives us a three-variable model, where variables *payment* (x_1), *risks* (x_2), and *benefits* (x_3) get the corresponding parameter values $\theta_1 = 4.72$, $\theta_2 = -.38$, $\theta_3 = .308$, and $b = 1.05$. Having included these additional variables, the explained variance is now somewhat improved (*Nagelkerke R^2* = .14), and the model classifies correctly 84.8% of the cases.

To further assess the sharing behaviour, we divided the data based on the sharing scenarios within the crowdsourcing tasks, illustrating the probability of accepting a location sharing job per payment in the four different scenarios. We modeled also these four cases independently as logistic regression. For the scenario *Trusted Advertiser*, for the variable *payment* (x_1) the parameter $\theta_1 = 9.31$ and $b = .32$, explaining nearly a quarter of the sharing behaviour (*Nagelkerke R^2* = .233). For the scenario *Untrusted Advertiser*, $\theta_1 = 3.987$ and $b = .131$, and (*Nagelkerke R^2* = .08). For the scenarios *Crowdee* and *Crowdee Users*, the model turned out to be not significant ($p = .051$). These as well as the total sharing rates are illustrated in Figure 3 as a function of payment. These results suggest that payment influences the location sharing behaviour mainly in the cases where the location would be also shared with an advertiser. Furthermore, when the
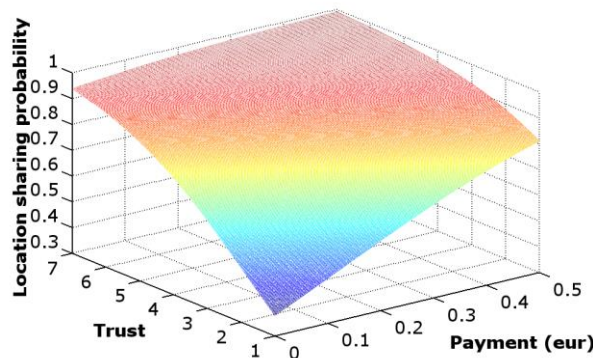
Figure 4. Location sharing probability as a function of trust and payment, in the scenario where the *untrusted advertiser* would also get the data. It can be seen that if the user has very high trust in the advertiser the sharing is very likely; however, trust was generally very low towards this advertiser.

advertiser is untrusted, the users are less likely to share a location, and a premium would need to be paid to reach the same sharing probability as in the case of a trusted advertiser.

To further assess the influence of trust, we added trust (towards the organization with which the location information would be shared) to each of the four models, illustrating the probability of accepting a location sharing job as a function of payment and trust. For the scenarios *Crowdee* and *Crowdee Users*, the model was not statistically significant ($p = .13$, and $p = .265$, respectively). In Table 2 are listed the parameters for the variables *payment* (x_1) and *trust* (x_2), describing the regressions in scenarios *Trusted* and *Untrusted Advertiser* as well as for the whole data set (with *overall trust* used as a variable x_2). As an illustration,
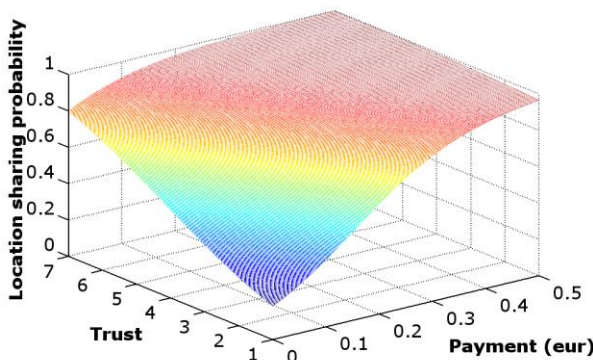

Figure 5. Location sharing in the scenario of sharing with a *trusted advertiser*, as a function of trust and payment. Higher acceptance rate is reached with a lower payment than in the scenario with *untrusted advertiser*.
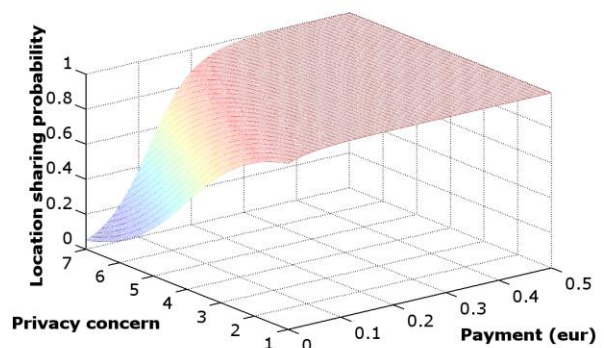

Figure 6. Total location sharing probability given as a logistic regression function of privacy concern measured as *desire for privacy* and the paid bonus in Euro.

the location sharing probability in the scenario *Untrusted Advertiser* is presented as a function of trust and payment in Figure 6, and that in the scenario *Trusted Advertiser* in Figure 5. Finally, the influence of privacy concern was assessed by modelling location sharing as a function of *payment* (x_1) and *desire for privacy* (x_2), cf. Figure 6.

The obtained parameter values were $\theta_1 = 24.24$, $\theta_2 = -.971$, and $b = 3.89$. The model could explain nearly half of the variance in the sharing behaviour (*Nagelkerke R^2 = .45*), and classify correctly 82% of the cases. The result suggests that privacy concern and payment have a strong influence on users sharing behaviour, cf. Figure 6.

5.3.2. Logarithmic modelling. Next, we take a deeper look at the results by considering the acceptance rate as percentages. We conducted a Kruskal-Wallis test, which confirmed the earlier results that there are differences in location sharing based on the scenario ($\chi^2(3) = 10.229$, $p = 0.017$). Further pair-

Table 3. The results of pair-wise Mann-Whitney U-tests, comparing the differences in location sharing rates in the four scenarios. Cells marked with a dash (-) are duplicates. Sharing in scenario *Untrusted Advertiser* differs significantly from the other scenarios, being in each case less frequent. No other statistically significant differences were found.

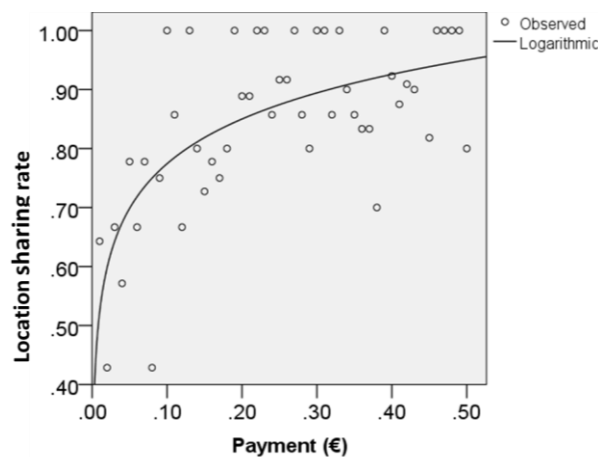|	Trusted Advertiser	Untrusted Advertiser	Crowdee	Crowdee Users
Trusted Advertiser	n.a.	$\chi^2 = 692.0$ $p = .005$	$\chi^2 = 973.0$ $p = .851$	$\chi^2 = 996.5$ $p = .862$
Untrusted Advertiser	-	n.a.	$\chi^2 = 669.5$ $p = .004$	$\chi^2 = 681.0$ $p = .004$
Crowdee	-	-	n.a.	$\chi^2 = 984.0$ $p = .948$

Figure 7. Location sharing frequency per payment on a crowdsourcing application follows a logarithmic model, where acceptance of a location sharing task increases from 40% to nearly 100% as the payment given for the task rises from 0€ to .50€.

wise Mann-Whitney U-tests with Bonferroni correction (the new alpha level being $\alpha = .0083$) showed less frequent location sharing in the scenario *Untrusted Advertiser* than in the other scenarios. This highlights that context seems to cause differences in location sharing behaviour even if the sharing rate is rather high. There are no notable differences in overall sharing frequencies between scenarios *Trusted Advertiser, Crowdee,* and *Crowdee Users.* The statistical results from the pair-wise comparisons are listed in **Error! Reference source not found.** These results do not take payment levels into consideration.

We assume that acceptance of a location-sharing task is dependent on the payment following a logarithmic model. This would mean that a higher payment yields higher sharing until, when reaching a certain threshold, plateaus. With this assumption, we take the percentage of accepted tasks for each payment level and fit this data on a logarithmic model. This gives a prediction showing the percentage of users sharing their location for a given price, as illustrated in Figure 7. We find that payment explains a significant proportion of the sharing behaviour, $R^2 = .44$, $p < .001$.

6. Discussion

We conducted an empirical study assessing users' location valuations on a mobile crowdsourcing platform. The results suggest that the majority of users reveal their location in all situations, even when not compensated for the extra information, and thus get no obvious benefit from doing so. This finding is quite similar to the one stated previously by Rose [15].

However, despite of being very compliant, differences in location valuation patterns can be found. The results show an increasing willingness to share with an increasing payment. Perceived benefits seem to affect location sharing positively, while risk perception as well as privacy concern seem to have a negative impact. Furthermore, our results suggest that the found differences in sharing patterns stem from varying trust – the users are less willing to share if the location is shared with an instance that they do not trust. These differences are discussed in the following subsections.

6.1. Location sharing with third parties: *Trusted Advertiser*

In the two scenarios of sharing with advertisers, the participants were not explicitly told which companies or organizations might get access to the location data. Instead, they were explained that their data would be shared with third parties such as advertisers. On the page that showed their location on a map and where the participant could choose to either share their location or not to share, an advert by an untrusted advertiser was shown in a prominent location. We find that the disclosing rate is significantly higher in this scenario compared to the one with an untrusted advertiser. Thus, it seems that there is granularity in location valuations with respect to sharing with advertisers. Also, interestingly, the overall disclosing rate does not differ statistically from the scenarios where sharing happens with *Crowdee* or other *Crowdee Users.* However, whereas in the scenarios *Crowdee* and *Crowdee Users* the sharing does not depend on the payment, in the scenarios where an advertiser is involved it does. This suggests that sharing in this situation is not solely due to benevolence. The users start possibly thinking of location sharing as a transaction; not only in terms of compromising privacy in exchange of a gained service, but also in terms of *how much is the location information worth*. In an earlier study, the users were willing to pay a small premium for enhanced privacy [16]. In our case, the users seem to accept a more privacy-intrusive situation if they get a small monetary bonus for it.

6.2. Location sharing with third parties: *Untrusted Advertiser*

In this scenario, there was an advert shown at the time of the location sharing task by an advertiser of low trustworthiness. From our results, showing that in this scenario the users were less willing to disclose location than otherwise, we can assume that the participants did consider the possibility of this

particular advertiser getting access to their location data. The users seem to require a small premium to share their location in this scenario in comparison to other disclosing situations. This result highlights that, even if the differences are small, the users do evaluate the value of their location data, possibly based on the risks that they perceive being involved in sharing.

6.3. Location sharing with other *Crowdee Users*

In the scenario of sharing in a social situation, the participant was shown on a map profile cards of "other users" in the area. Our hypothesis was that the participants would think twice about location sharing if it also has social implications, and we expected to see lower sharing scores in this scenario. This did not happen, which could be also due to the fact that the location would not be shared with any users in the participants' actual social circles, but with strangers. Another explanation would be that users have a tendency to feel like they belong to a group (in this case the Crowdee users), and favor the other individuals who belong to the group [32].

6.4. Location sharing in general

In our study, we could explain up to nearly 50% of the variance in location sharing behaviour by the given payment, or with a model combining the payment and trust or privacy concern. Perceived risks and benefits were also found to influence location sharing, however, assessing what their contribution to the total sharing model is would require a larger data set. Trust and privacy concern are strongly correlated – it seems like a plausible explanation for the sharing patterns that if a user trusts the instance they are asked to share location with no privacy concern are present, and sharing is very likely. Also vice versa: mistrust towards an advertiser provokes privacy concern, and inhibits sharing.

Multiple other variables are likely to play a role when deciding on whether to disclose location or not. For example, we did not consider the effect of the physical location on the disclosure rate. Based on earlier studies, users are more willing to share a location if it has a large and diverge set of visitors [20]. For example, users might be more willing to share their location if they are in the city, and less so if they are at home.

7. Limitations

Using a crowdsourcing platform allowed for studying the effect of price in a realistic scenario without the need to resort to asking users about the price hypothetically, making the platform a well working solution for addressing the problem. However, our results might be specific to crowd workers, and in particular, the users of the crowdsourcing platform used in this study. Repeating the study with another platform would shed light on the reliability of the results.

Volunteered information might fundamentally differ from information that is collected for example through ambient sensors. This leads to certain populations being overly represented in the data as some groups do not voluntarily disclose information [33].

Disclosure using LBS is not necessarily so straightforward that the user could make a fully informed decision about the benefit-privacy transaction. It can be that the user is not fully knowledgeable about the disclosure in the first place. Even more importantly than that, once the disclosure has happened, the user has no way of knowing what happens to the data – about the possible subsequent use of the data, how it is being analyzed and aggregated with other information, and distributed to other parties. This leads to anxiety of control over one's personal information [10], to loss of contextual integrity when the information is handled and distributed contrary to the users' expectations [9], and to powerlessness in the absence of a reasonable, privacy preserving choice [29]. This study, however, did not take into account the complexity of location sharing, but made a simplification and assumed that the decision to share or not to share a location depends mainly on who is asking (and why), as well on the given payment. The further analysis of the awareness of the information flow the user has in the disclosure situation remains a topic for further studies.

Also, considering the high number of times the users might, either purposely or unknowingly disclose their location to different parties throughout the day, it is highly unlikely that in each of these events the ratio of received benefits and privacy cost would be systematically evaluated by the user, let alone assessing the possible long term impact of a disclosure. Therefore, the results cannot be directly generalized.

8. Conclusions

We conducted a study examining location valuations in one-time sharing situations using a mobile crowdsourcing platform. We find that the sharing scenario, as well as the paid amount, influence the sharing of location. However, the payment is found to have an impact mainly in the scenarios where the location would also be shared with advertisers, even though the needed payment to compensate for the location sharing seems to be minimal. Also trust,

perceived benefits and risks, as well as privacy concern influence the users' willingness to share location. We conclude that users are very compliant and accept sharing their location in most cases, an exception being sharing with an untrusted advertiser. A more privacy-intrusive situation is accepted for a small extra payment.

Acknowledgements

References

[1]   J. Y. Tsai, P. G. Kelley, L. F. Cranor, and N. Sadeh, "Location-Sharing Technologies : Privacy Risks and Controls," *A J. Law Policy Inf. Soc.*, vol. 6, no. 2, pp. 119–151, 2010.

[2]   A. Goldfarb and C. Tucker, "Online Display Advertising: Targeting and Obtrusiveness," *Mark. Sci.*, vol. 30, no. 3, pp. 413–415, 2011.

[3]   M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs," *Pers. Ubiquitous Comput.*, vol. 15, no. 7, pp. 679–694, 2011.

[4]   N. Ozer, C. Conley, D. H. O'Connell, T. R. Gubins, and E. Ginsburg, "Location-Based Services: Time for a Privacy Check-In," *SSRN Electron. J.*, 2010.

[5]   B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sci.*, vol. 9, no. 2, pp. 127–152, 1978.

[6]   I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2. pp. 179–211, 1991.

[7]   D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A study on the value of location privacy," *Proc. 5th ACM Work. Priv. Electron. Soc.*, pp. 109–118, 2006.

[8]   J. Crampton, "The Ethics of GIS," *Cartogr. Geogr. Inf. Sci.*, vol. 22, no. 1, pp. 84–89, 1995.

[9]   H. Nissenbaum, "Privacy as contextual integrity," *Washingt. Law Rev.*, vol. 79, no. 1, pp. 101–139, 2004.

[10]   A. Leszczynski, "Spatial big data and anxieties of control," *Environ. Plan. D Soc. Sp.*, vol. 33, no. 6, pp. 965–984, 2015.

[11]   M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, no. 1. pp. 104–115,

1999.

[12]   T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006.

[13]   S. Preibusch, "Guide to measuring privacy concern: Review of survey and observational instruments," *Int. J. Hum. Comput. Stud.*, vol. 71, no. 12, pp. 1133–1143, 2013.

[14]   P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *J. Consum. Aff.*, vol. 41, no. 1, pp. 100–126, 2007.

[15]   E. Rose, "Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?," *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci.*, 2005.

[16]   J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research*, vol. 22, no. 2. pp. 254–268, 2011.

[17]   A. Acquisti, L. K. John, and G. Loewenstein, "What Is Privacy Worth?," *J. Legal Stud.*, vol. 42, no. 2, pp. 249–274, 2013.

[18]   L. K. John, A. Acquisti, and G. Loewenstein, "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *J. Consum. Res.*, vol. 37, no. 5, pp. 858–873, 2011.

[19]   A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, vol. 3, no. 1. pp. 26–33, 2005.

[20]   E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh, "Empirical models of privacy in location sharing," *Proc. 12th ACM Int. Conf. Ubiquitous Comput. - Ubicomp '10*, p. 129, 2010.

[21]   G. Danezis, S. Lewis, and R. Anderson, "How much is location privacy worth?," *Fourth Work. Econ. Inf. Secur.*, vol. 78, pp. 739–748, 2005.

[22]   O. Barak, G. Cohen, a Gazit, and E. Toch, "The price is right?: economic value of location sharing," *2nd ACM Int. Work. Mob. Syst. Comput. Soc. Sci.*, pp. 891–899, 2013.

[23]   a. J. B. Brush, J. Krumm, and J. Scott, "Exploring end user preferences for location obfuscation, location-based services, and the value of location," *Proc. 12th ACM Int. Conf. Ubiquitous Comput. - Ubicomp '10*, p. 95, 2010.

[24]   H. J. Smith, T. Dinev, and H. Xu, "Theory and Review Information Privacy Research: an Interdisciplinary Review 1," *MIS QuarterlyInformation Priv. Res.*, vol. 35, no. 4, pp. 989–1015, 2011.

[25]   H. Xu, H. Teo, and B. C. Y. Tan, "Predicting the adoption of location-based services: the role of trust and perceived privacy risk," *Proc. 26th Int. Conf. Inf. Syst. (ICIS 2005), Las Vegas*, no. Beinat 2001, pp. 897–910, 2005.

[26]   L. Barkhuus, "Privacy in Location-Based Services , Concern vs . Coolness," in *Proc. of MobileHCI 2004*, 2004.

[27] P. Xu, Heng; Gupta, Sumeet; Shi, "Balancing User Privacy Concerns in the Adoption of Location-Based Services : An Empirical Analysis across Pull-Based and Push-Based Applications," 2009.

[28] B. Naderi, T. Polzehl, A. Beyer, T. Pilz, and S. Möller, "Crowdee: mobile crowdsourcing micro-task platform for celebrating the diversity of languages.," in *INTERSPEECH*, 2014, pp. 1496–1497.

[29] M. Poikela and F. Kaiser, "'It Is a Topic That Confuses Me' – Privacy Perceptions in Usage of Location-Based Applications," in *European Workshop on Usable Security (EuroUSEC)*, 2016.

[30] Center for Leadership and Values in Society (CLVS-HSG) of the University of St.Gallen, "Public Value Atlas," 2015. [Online]. Available: http://www.gemeinwohlatlas.de/en/atlas. [Accessed: 01-Apr-2016].

[31] A. Morton, "Measuring Inherent Privacy Concern and Desire for Privacy-A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern.," in *International Conference on Social Computing(SocialCom)*, 2013.

[32] H. Taijfel, "Experiments in intergroup discrimination.," *Sci. Am.*, vol. 223, no. 5, pp. 96–102, 1970.

[33] C. M. Dalton, L. Taylor, and J. Thatcher, "Critical Data Studies: A Dialog on Data and Space," *Big Data Soc.*, pp. 1–9, 2016.

Appendix

In the following scales, the items that were inverted prior to analysis in order to match with the scale direction are marked with an asterisk (*). The question order was randomized.

A1. Location-Based Services Risks Scale
1. I believe that there are no risks involved when mobile applications collect location information that is anonymous. *
2. I believe that mobile applications track users' location only if it is required for their functionality. *
3. I am worried that using location-based applications would lead to unsolicited marketing.
4. I am worried that if I use location-based applications, I might get tracked by the government.
5. Using location-based applications involves the risk of getting stalked.
6. I am worried that using location-based applications would lead to my home location being revealed.
7. I am worried that using location-based applications involves the risk of becoming a victim of identity theft.
8. I am worried that if I use location-based applications, strangers might know too much about my activities.
9. Using location-based applications poses a threat to my personal safety.

A2. Location-Based Services Benefits Scale
1. Using location-based services is practical.
2. Using location-based applications is useful.
3. Using location-based applications enables me to accomplish tasks more quickly.
4. Using location-based applications is fun.
5. Using location-based applications makes communication faster.
6. Using location-based applications simplifies communication.
7. Location-based applications enhance my social life. (*This item was left out of the final analysis because it deteriorated the internal consistency of the scale.*)

A3. Location-Based Services Normative Beliefs Scale
1. People who I care about and who care about me think that I should use location-based applications.
2. People who are important to me think that I should use location-based applications.
3. Everybody uses location-based applications. (*This item was left out of the final analysis because it deteriorated the internal consistency of the scale.*)
4. People who I care about and who care about me think that there are certain benefits in using location-based applications.

A4. Dispositional Privacy Concern Scale
1. It is the most important thing for me to protect my privacy.
2. I'm comfortable telling other people, including strangers, personal information about myself. *
3. I try to minimize the number of times I have to provide personal information about myself.
4. I am comfortable sharing information about myself with other people unless they give me reason not to. *
5. I have nothing to hide, so I am comfortable with people knowing personal information about me. *
6. I try to change the topic of a conversation if people start asking too much about me.

A5. Trustworthiness Scale
These questions were repeated for each of the four instances with whom the location would be shared (altogether 16 questions).

1. How trustworthy do you find <the instance with whom the location would be shared>?
2. How reliable do you find <the instance with whom the location would be shared>?
3. In general, how risky do you find it to give location information to <the instance with whom the location would be shared>?
4. How concerned are you that <the instance with whom the location would be shared> could harm you if it had your location data?