Location-Based Applications - Benefits, Risks, and Concerns as Usage Predictors

Maija Poikela Ina Wechsung Sebastian Möller
Quality and Usability Lab, Telekom Innovation Laboratories, TU Berlin
firstname.lastname@telekom.de

ABSTRACT

Location-based applications offer various benefits to users, but at the cost of putting one's privacy at risk. When deciding on whether to use these applications or not, the user has to perform a risk-benefit analysis based on the available knowledge on the apps' information privacy practices. Users can take some measures to protect themselves from the risks, but concern might also discourage adoption of location-based technologies. In this paper, we show that perceived risks dictate the usage of location-based applications. Perceived benefits seem to influence how often location-based applications are installed, but not how often they are used. According to our results, awareness of such applications' information privacy practices has an influence on whether or not the user installs these applications, but does not influence their usage. We also show that users with high privacy concern are less likely to install location-based applications than others; however, privacy concern was not found to correlate with use of location-based applications, or with protective behavior.

1. INTRODUCTION

The last decade has seen a wide range of location-based applications (LBA) in areas such as communication, self-expression, or navigation [1], [2]. Users have several benefits from using LBA, such as finding nearby services, getting discounts, or informing others about their whereabouts [3]. Besides the benefits, using LBA also introduces risks for the user, including identity theft, location-based adverts, being stalked, electronic surveillance, and being maliciously tracked [2].

With various technologies, the user needs to perform careful risk-benefit analysis with the information at hand and decide whether to use the service [4], sometimes at the cost of (location) privacy [5]. In order to protect oneself, the user can decide to share her location only with people or organizations she trusts, not to use some services, or switch the location services completely off, thereby making some services unusable. In order to properly assess the risks, the user needs to be aware of how the various applications handle the users' data. This evaluation of benefits and risks is known in the privacy literature as *privacy calculus* [6]. According to some studies, however, the privacy calculus does not hold but the users seem to have a tendency to excessively value immediate benefits and overlook future privacy risks [7].

In pursuit of evaluating what dictates privacy concern and likelihood to engage in behavior to protect one's privacy, previous literature assesses dispositional and other personal characteristics. According to Westin's categorization [8], consumers can be divided into *Privacy Fundamentalists (25%), Pragmatics (57%),* and *Unconcerned (18%).* These categories represent dispositional values, and are not expected to change greatly over time. While other studies show that inherent characteristics, such as general "closeness to the world" [9], and personality differences [10], correlate with privacy related behavior, some critique has lately emerged on the predictive power of the Westin's segmentation [11]. Other work has assessed privacy concern and protective behavior, relating these with age, gender, and education, e.g. [12].

When assessing the interplay between privacy awareness, trust, and app usage, four basic user types could be identified:

1) The user has low awareness of app's data privacy practices as well as low trust towards the company behind the app, which leads to high privacy concern and less usage of the app.
2) The user has low awareness and high trust, leading to low privacy concern and increased usage of the app.
3) The user has high level of awareness, and the app's inadequate data privacy practices lead to high privacy concern and less usage of the app.
4) The user has high level of awareness, and the app's good data privacy practices lead to low privacy concern and increased usage of the app.

These privacy personas were discussed with similar inferences by Spears and Sheena [13], where the 'Nothing to Hide' persona would correspond to case 2 in this presentation.

The privacy literature presents many attempts at measuring individuals' privacy concern. One of the most influential ones is the *Internet Users' Information Privacy Concern* scale (IUIPC) by Malhotra [14]. While IUIPC measures concern towards organizational privacy practices in the context of the Internet, it is unclear how well it adapts to the mobile context. Morton et al. [15] present a construct called *Desire for Privacy* (DFP) as part of a measure for *Dispositional Privacy Concern* (DPC). DFP is reportedly positively related to IUIPC [15], and could explain the dispositional component of privacy concern, i.e. the part that does not take context into consideration.

In this paper, we evaluate how dispositional privacy concern, awareness of apps' data privacy practices, and perception of risks and benefits of LBA affect the use of such applications. These aspects were assessed in two studies during December 2014. We begin in Section 2 with assessing the effect of dispositional privacy concern, and that of the perceived risks and benefits of using LBA, on the usage of such applications on smartphones as

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22-24, 2015, Ottawa, Canada.

well as on protection behavior. In Section 3, we assess the correlation between the level of being informed about apps' information privacy practices and privacy concern. In Section 4, based on the data from both these studies, we analyze the correlation between privacy concern and risk and benefit perception. Finally, these findings are discussed in Section 5, followed by a summary of the results.

2. STUDY 1: USE OF LOCATION-BASED APPLICATIONS

To study the use of location-based applications and how this correlates with the perceived risks and benefits of using these applications, and with privacy concern, a survey study with 19 smartphone owners was conducted.

2.1 Measures

Dispositional Privacy Concern. To measure the participants' dispositional privacy concern, the six-item construct called *Desire for Privacy* (DFP) by Morton [15] with a seven-point end-labelled answer scale anchored with "*strongly disagree*" and "*strongly agree*", was used. Three of the items were inverted before the analysis to give the mean value of these items as an overall privacy concern score, where a higher value denotes higher privacy concern. To check the internal consistency, we calculated Cronbach's α. The scale showed acceptable consistency, and after removing two items, was improved to good internal consistency, (Cronbach's α = .72). We used this four-item scale for analyzing users' privacy concern.

Risk Perception. We included a 13-item *Risk Perception* scale measuring perceived risks using location-based services. Most of the items regarding the risks were based on an earlier study by Tsai et al. [2], including items such as "Using location-based applications involves the risk of getting stalked.", and "I am worried that if I use location-based applications, I might get tracked by the government." Some items were added, such as "Using location-based applications poses a threat to my personal safety."

The 13 risk-related items were used to compute an overall risk perception score, the mean value of the 13 items. Two of the items were inverted before the analysis so that a higher score with this construct would denote a higher level of risk perception. A seven-point end-labelled answer scale anchored with "*fully disagree*" and "*fully agree*" was used. The scale showed good internal consistency (Cronbach's α = .85).

Benefit Perception. To measure the extent to which users see benefits in using location-based services, we included a four-item *Benefit Perception* scale. Two of the items were from literature ("Using location-based applications is useful", "Using location-based applications enables me to accomplish tasks more quickly") [3]. Additionally, we added two more items for the benefits scale.

These benefit-related items were used similarly as in the risk perception scale to calculate a score for perceived benefits. Again, a seven-point end-labelled answer scale anchored with "*fully disagree*" and "*fully agree*" was used. We found that the scale showed acceptable internal consistency (Cronbach's α = .69). However, after removing one item, the remaining three-item scale showed good internal consistency (Cronbach's α = .79), and was used for analysis.

Usage Frequency of Location-Based Services. The participants were asked how often they used certain apps with location-sharing functionalities. The apps within the three-item *LB-App Usage Frequency* scale included Facebook, WhatsApp, and a navigation app. The usage of these apps was graded on a 6-point answer scale: "*daily*" ('5'), *"several times a week"* ('4'), "*several times a month"* ('3'), *"more seldom"* ('2'), and "*never*" ('1'), '0' denoting "*not installed*". The mean value is used for analysis, and referred to later as the *LB-App Usage Frequency* score.

Protective Behavior. Additionally, we studied the protection measures the users take to ensure their location privacy. For this, a *Protective Behavior* scale with three items on a binary answer scale ("*yes*" / "*no*") was added. The scale included the following items: "Are location services enabled on your smartphone?", "Are you using apps, for which you know that they are accessing your location data also when the app is not open?", and "Have you ever installed and used an app which accessed your location and you didn't know why?". All of the items were inverted such that a higher mean score on this scale denotes more intense protective behavior. The scale showed acceptable internal consistency (Cronbach's α = .61).

Demographics. As demographic data, we asked the participants for their age, education level, occupation, and gender.

2.2 Results

In total 25 participants were recruited for the study, and given the paper questionnaires together with a short briefing to the study. We collected 19 responses (11 male, 8 female); six were not returned on time. The participation was voluntary and no incentives were given. The participants' age ranged from 22 to 60 years, with a mean of 34.2 years. 11% of them were students, and 95% employed. 16% had a secondary degree, 26% a high-school degree, and 55% had a university degree. 42% of the participants were female.

Correlations were computed between the *LB-App Usage Frequency* and the constructs *Dispositional Privacy Concern*, *Risk Perception*, and *Benefit Perception*. We used Cohen's [16] suggestions throughout the analysis for interpreting the effect size. For any of the variables normality of the distribution could not be assumed, and Spearman's rho was used.

A strong negative correlation was found between *Risk Perception* and *LB-App Usage Frequency*, $r_s(17)=-.57$, $p=.005$. However, no significant correlation was found between *LB-App Usage Frequency* and *Benefit Perception*. Also, the correlation between *LB-App Usage Frequency* and *Dispositional Privacy Concern* did not turn out to be significant. This suggests that how often location-based apps are used is affected by perceived risks, but according to these results, not by perceived benefits nor by the privacy concern inherent to the user.

Similarly, the Spearman's rank correlations for *Protective Behavior* with *Dispositional Privacy Concern*, *Risk Perception*, and *Benefit Perception* were calculated. Spearman's rho shows a strong correlation between *Protective Behavior* and *Risk Perception*, $r_s(17)=.72$, $p<.001$. *Protective Behavior* on the contrary does not correlate with *Benefit Perception*, or with *Dispositional Privacy Concern*. As a summary, how much privacy protection measures the user takes on her mobile phone seems to correlate with perceived risks, but not with the perceived benefits, nor with the privacy concern. The results are presented in Table 1.

Table 1: Effect sizes of the correlations found in the two studies, with the corresponding study (S1, S2, or a combination) marked in brackets. The p-values are reported below each correlation. The items marked with an asterisk (*) are behavioral items. For visualization purposes, negative correlations are marked with red, and positive with green color. Only significant correlations are reported; results that were not significant are marked with a dash (-). An empty cell denotes that the correlation has not been checked.

	Dispositional Privacy Concern	*Awareness*	*Risk Perception*	*Benefit Perception*	*Gender*	*LBS-App Usage Frequency**	*LB-App Installed**	*Protective Behavior**
Dispositional Privacy Concern		- (S2)	r(84)=.37 p<.001 (S1 & S2)	- (S1 & S2)	- (S1 & S2)	- (S1)	r(84)=-.33 p=.002 (S1 & S2)	- (S1)
Awareness	duplicate		- (S2)	- (S2)			r_s(66)=.27 p=.013 (S2)	
Risk Perception	duplicate	duplicate				r_s(17)=-.57 p=.005 (S1)	r(84)=-.30 p=.002 (S1 & S2)	r_s(17)=.72 p<.001 (S1)
Benefit Perception	duplicate	duplicate				- (S1)	r(84)=.28 p=.004 (S1 & S2)	- (S1)
Age	r_s(85)=.26 p=.016 (S1 & S2)					r_s(85)=-.40, p<001 (S1 & S2)		

3. STUDY 2: AWARENESS OF APPS' INFORMATION PRIVACY PRACTICES

To study the extent to which smartphone users are aware of how apps share their data, an online questionnaire with 68 participants was conducted.

3.1 Measures

Privacy Concern, Risk and Benefit Perception. *Dispositional Privacy Concern*, *Risk Perception*, and *Benefit Perception* were measured and treated as in Study 1 (see Section 2.1).

Awareness of Apps' Information Usage Practices. The online study included a 15-item *Awareness* scale measuring the users' knowledge of the data privacy practices of Facebook, WhatsApp, and a navigation app. For each of these apps, the participants were asked five questions on a binary ("*yes*" / "*no*") scale which of the statements, according to their best knowledge, held true:

The application in question…

- knows the users' location
- gives the user's location away to third parties
- has access to the address book
- has access to device memory
- has access to camera.

The results for one of the questions regarding the navigation app were highly inconsistent with the rest of the scale, and this item was left out of the analysis. The now 14-item scale showed good internal consistency (Cronbach's $\alpha = .71$).

Installing Applications. To see how the above mentioned awareness correlates with behavior, we also asked whether the users had the three apps (Facebook, WhatsApp, a navigation app) installed on their smartphones. We call this construct *LB-Apps Installed.*

Demographics. As demographic data, we asked for participants' age on 5 years intervals. Additionally, we asked for education level, occupation, and gender.

3.2 Results

In total 96 participants' responses were collected. 68 of these were finally analyzed (28 non-smartphone users or incomplete responses were disqualified). The study was conducted as an online questionnaire using the open source tool Limesurvey, to which the participants were found mostly through social media sites. The participants received no incentives. The participants' age ranged from 18-22 to 53-57 years, with a median age group of 23-27 years. The occupational distribution was as follows: 57% students, 37% employed or interns, 3% self-employed, and 3% unemployed. 6% of the participants had a secondary degree, 68% a high-school degree, and 26% a university degree. 41% of the participants were female.

To study whether *Awareness* correlates with *Dispositional Privacy Concern*, Spearman's rho was used, because the assumptions of normality could not be met for either of the variables. Spearman's rho was also used for calculating the correlation between *Awareness* and *Risk Perception*, and *Awareness* and *Benefit Perception.* There was no correlation found between *Awareness* and *Dispositional Privacy Concern*, or with *Awareness* and *Risk* or *Benefit Perception.*

Finally, correlation between *Awareness* and *LB-Apps Installed* was calculated, again using Spearman's rho, which showed a weak correlation, $r_s(66)=.27$, $p=.013$.

4. RISK AND BENEFIT PERCEPTION, AND PRIVACY CONCERN

To study how users' privacy concern correlates with the risks and benefits they see in using location-based applications, we combined the data from the two studies. With this larger data set, we could address the issue of the small sample size in Study 1.

4.1 Measures

Privacy Concern, Risk and Benefit Perception. Also in this part of the study, *Dispositional Privacy Concern*, *Risk Perception*, and *Benefit Perception* were measured and treated as in Study 1 (see Section 2.1). We conducted a Levene's test to measure whether the variances of the *Dispositional Privacy Concern* differ between Study 1 and Study 2, and then, an independent samples t-test to check for differences in the mean values. These showed no significant difference, F=.47, p=*.497;* t(85) = 1.13, p=.269. We then repeated this for *Risk Perception*; no differences were found, F=.85, p=.360; t(85)=-.87, p=.389. For *Benefit Perception* normality of variance could not be assumed, and a Mann-Whitney U-test was used to compare the means, F=.31, p=.581; U=642, p=.971. No differences were found, and thus, for all these sample pairs, we can assume them to come from the same population.

Installing Location-Based Applications. We computed a new binary variable that denotes whether an app is installed or not, for each of the apps included in the *LB-App Usage Frequency* construct in Study 1 by considering when the *LB-App Usage Frequency* got a value different from '0', denoting "not installed". We could then combine this score with the *LB-App Installed* construct in Study 2. Independent samples t-test showed no significant difference between the Studies 1 and 2 for *LB-App Installed*, t(85)=.22, p=.825.

Demographics. As demographic data, age, education level, and gender were included from both the studies. We grouped all the participants in Study 1 into age groups in 5 years' intervals (group '0' denoting the age group of under 18yrs, '1' = 18-22yrs, '2' = 23-27yrs etc.), following the grouping in the Study 2. We used Mann-Whitney U-test to study the age distribution between the two studies, and found that the participants in the Study 1 were significantly older, U=370, p=.003.

4.2 Results

To measure the correlation between *Dispositional Privacy Concern* and *Risk Perception*, we used Pearson's r, which showed a moderate positive correlation, r(85)=.37, p<.001. Pearson's r showed no correlation between *Dispositional Privacy Concern* and *Benefit Perception*. According to these results it seems that the users with high privacy concern expect using location-based application to bring some risks.

The correlation between *Risk Perception* and *LB-Apps Installed*, as well as between *Benefit Perception* and *LB-Apps Installed*, was computed using Pearson's r. Between *LB-Apps Installed* and *Risk Perception*, a moderate negative correlation was found, r(85)=-.30, p=.002. Pearson's r showed a moderate positive correlation between *LB-Apps Installed* and *Benefit Perception*, r(85)=.28, p=.004. A moderate negative correlation was found between *LB-Apps Installed* and *Dispositional Privacy Concern*, r(85)=.-33, p=.002.

The correlation of age on *Dispositional Privacy Concern* was calculated using Spearman's rho because normality could not be assumed for age. The results indicate that privacy concerns increase with age, r_s(85)=.26, p=.016. Similarly, using Spearman's rho, we find that younger participants are more likely to use LBA, r_s(85)=-.398, p<001. Finally, we calculated the differences between male and female participants on *Dispositional Privacy Concern* using an independent samples t-test; no differences were found, t(85)=.756, p=.474.

5. DISCUSSION

In this paper, we present two studies assessing how awareness of location-based applications' information privacy practices, privacy concern, and perception of benefits and risks on location-based services affect app usage and protective behavior. For visualization, the statistically significant correlations, together with the p-values, are presented in Table 1.

5.1 Perceived Risks and Benefits

We found a strong negative correlation between *Risk Perception* and *LB-App Usage Frequency:* The more risks users see in location based applications, the less they use them. A similar, albeit slightly weaker, effect can be seen with installing LBA. *Risk Perception* correlates strongly also with *Protective Behavior*, which could suggest that the more risks users see in location based applications, the more they take protective measures against these risks. While these results are not completely unexpected, this would imply that how much risks a user sees in location-based services would work as a rather good predictor, partly explaining behavior using these services.

Perceived risks seemed to have a strong effect and lead to less usage, whereas perceived benefits did not seem to lead to increased usage rate of LBA. However, a positive moderate correlation was found between the perceived benefits and the installation rate of LBA, and a moderate negative correlation between the perceived risks and the installation rate. These findings suggest that once the user has done a risk-benefit calculation and decided to install an application, the risks – rather than the benefits – dictate the decision on whether to use LBA. This result seems to be in line with the findings from an earlier study by Tsai et al. [2], concluding that the users report that the risks of using location-based services outweigh the benefits. Our questionnaire handles perceived benefit on a rather general level, and taking context into account – for example, the type of the app in question – might provide different results or perhaps better predictive power. Thus, this can be seen as an indicative result, and more research should be put into this topic to validate the result.

In our experimental setting that did not include a field study, it might be challenging for the users to imagine what the possible benefits of using a location-based application are without being in the actual context of use. This might be better to study in a setting where the users would see that they get some, preferably immediate, benefits for using a service.

5.2 Privacy Concern

Dispositional Privacy Concern had a moderate negative correlation with *LB-Apps Installed*, suggesting that the more privacy concerns a user has, the less inclined she is to install

applications. A similar finding has been presented by Xu et al. [17] in the context of location-based marketing, where customer privacy concern was seen as the major factor inhibiting adoption.

No correlations were found with *Dispositional Privacy Concern* and the other behavioral measures, namely using location based applications, or protective behavior. *Dispositional Privacy Concern* did, however, have a moderate positive correlation with *Risk Perception.* This could suggest that while *Dispositional Privacy Concern* might work as a predictor of perceiving risks, it has only low predictive power for behavioral measures. This result could suggest that even the users who are fundamentally concerned about their privacy could adopt location-based applications if they are convinced that the possible risks of using them are minimal.

We found that the users' dispositional privacy concern increases with age, and that younger participants used location-based applications more. This is in line with an earlier finding by Sheehan [12], who stated that younger users are rather pragmatic in their online behaviors.

5.3 Awareness of Data Privacy Practices

We found, contrary to our assumptions, that awareness of applications' information privacy practices does not correlate, or correlates only weakly, with behavior, privacy concern, or risk and benefit perception. The fact that we could not empirically verify the different privacy personas based on the awareness within our study does not verify the absence of such personas. Further studies are required to assess the influence of awareness and trust on application usage in order to identify the full phenomenon.

5.4 Implications for privacy segmentation

This paper does not end the debate on privacy segmentation, but does suggest that there are multiple factors that seem to have an effect on behavior. Some of these factors are likely to be independent of the context, such as age, and dispositional privacy concern. However, our results suggest that there are a multitude of context-dependent factors that seem to have a strong effect on the installation and usage of apps, as well as on protection behavior. These results pinpoint that care should be taken when creating privacy personas, as many factors, including the risks the users see, might have an even stronger impact on application usage than privacy concern.

5.5 Limitations

The two studies presented in this paper were questionnaire studies, the first one conducted as a paper questionnaire, and the second one as an online questionnaire. A possibility of response bias exists as a result of self-reporting, which might influence the validity of these results. For example, a consequence of this bias might be that these results possibly show more protection behavior than in reality.

The participants for the second study were recruited mainly through social media sites, which might produce a biased sample. Our participants might be more likely to be users of the Facebook app, and, are possibly also otherwise active social media users who might be more likely to use messaging apps such as WhatsApp. This could skew the results regarding the application installing rate, as well as app usage rate. The study should be repeated with a different sample to account for this possible bias.

In this study, we have considered usage on the scale from "not installed" to "daily". This score might be biased by the users who have not installed the application, and leaving those users out from the analysis would be an option.

This study is simplified in that it considers Facebook and WhatsApp as location-based applications. While the user can take some measures to protect one's location privacy, such as switch off the location services, or use specific Apps to deny other Apps the permission to access one's location (e.g. [18]), for example Android phones deal with the permissions as an adamant dichotomous decision which one has to comply with to install Apps [19]. A topic for future studies would be to take also into consideration whether some such privacy protection mechanisms are in place, as it might also influence how comfortable users feel about using apps and sharing information with them.

6. CONCLUSIONS

Our results suggest that installing location-based applications might be an outcome of privacy calculus, where a user analyses the foreseeable benefits and risks, being influenced also by her general privacy concern and awareness on the apps' information privacy practices. Whether or not the applications are finally used seems to depend on to what extent the user believes that risks are involved. According to our study, perception of risk on location-based applications is likely to lead also to increased protective behavior.

7. ACKNOWLEDGEMENTS

We would like to show our gratitude to Vera Burckhardt, Tim Coen, Robert Greinacher, Sebastian Kraus, Christopher Krügelstein, Eridy Lukau, Domenic Reuschel, Charlotte Spang, and Marius Wessel for their contributions in conducting the experiments, as well as to the participants for their valuable time. Finally, we thank Dr. Rahul Swaminathan for his helpful comments and feedback.

8. REFERENCES

[1] K. Tang, J. Lin, and J. Hong, "Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing," *Proc. 12th ACM Int. Conf. Ubiquitous Comput. - Ubicomp '10*, vol. 12, no. 4–5, pp. 85–94, 2010.

[2] 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.

[3] 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.

[4] 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.

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

[6] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti, "Privacy calculus model in e-commerce – a study of Italy and the United States," *European Journal of Information Systems*, vol. 15, no. 4. pp. 389–402, 2006.

[7] A. Acquisti, "Privacy in electronic commerce and the economics of immediate gratification," in *5th ACM conference on Electronic Commerce*, 2004, p. 21.

[8] P. Kumaraguru and L. Cranor, "Privacy indexes: A survey of westin's studies," *Science (80-.).*, vol. Tech. rep., no. December, pp. 1–22, 2005.

[9] M. Poikela, R. Schmidt, I. Wechsung, and S. Möller, "Locate!-When do Users Disclose Location?," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[10] G. Bansal, F. M. Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decis. Support Syst.*, vol. 49, no. 2, pp. 138–150, 2010.

[11] A. Woodruff, V. Pihur, S. Consolvo, L. Schnidt, L. Brandimarte, and A. Acquisti, "Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014, pp. 1–18.

[12] K. B. Sheehan, "Toward a Typology of Internet Users and Online Privacy Concerns," *The Information Society*, vol. 18, no. 1. pp. 21–32, 2002.

[13] J. L. Spears and L. E. Sheena, "'I have nothing to hide; thus nothing to fear': Defining a Framework for Examining the 'Nothing to Hide' Persona," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[14] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, vol. 15, no. 4. pp. 336–355, 2004.

[15] 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.

[16] J. Cohen, "A power primer.," *Psychol. Bull.*, vol. 112, no. 1, pp. 155–159, 1992.

[17] H. Xu, X. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decis. Support Syst.*, vol. 51, no. 1, pp. 42–52, 2011.

[18] S. (Stericson), "Google play - Permissions Denied," 2013. [Online]. Available: https://play.google.com/store/apps/details?id=com.stericson.permissions.donate&hl=en.

[19] Google, "Google Play Help - About app permissions." [Online]. Available: https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1. [Accessed: 10-Jun-2015].

9. APPENDIX

Dispositional Privacy Concern

It is the most important thing for me to protect my privacy.

I'm comfortable telling other people, including strangers, personal information about myself.

I try to minimize the number of times I have to provide personal information about myself.

I am comfortable sharing information about myself with other people unless they give me reason not to.

I have nothing to hide, so I am comfortable with people knowing personal information about me.

I try to change the topic of a conversation if people start asking too much about me.

Risk Perception

Using location-based applications is risky.

Using location-based applications involves the risk of getting stalked.

I am worried that using location-based applications would lead to my home location being revealed.

I am worried that if I use location-based applications, I might get tracked by my boss.

I am worried that if I use location-based applications, I might get tracked by the government.

I am worried that using location-based applications would lead to unsolicited marketing.

I am worried that using location-based applications involves the risk of becoming a victim of identity theft.

I am worried that if I use location-based applications, strangers might know too much about my activities.

Using location-based applications poses a threat to my personal safety.

I believe that there are no risks involved when mobile applications collect location information that is anonymous.

I believe that companies behind mobile applications are interested in selling my location data for marketing purposes.

I believe that within my circles, there are no victims of phone surveillance.

I believe that mobile applications track users' location only if it is required for their functionality.

Benefit Perception

Using location-based applications is fun.

Using location-based services is practical.

Using location-based applications is useful.

Using location-based applications enables me to accomplish tasks more quickly.

Protective Behavior

Are location services enabled on your smartphone?

Are you using apps, for which you know that they are accessing your location data also when the app is not open?

Do you allow all apps unrestricted access to your location data?

Do you inform yourself with the app provider (Web site, Forum), how exactly your location data is used?

Have you ever decided not to install an app because it requires access to your location?

Have you ever turned off your phone in order to keep your location information private?

Have you ever installed and used an app which accessed your location and you didn't know why?