A Comparison of Privacy and Security Knowledge and Privacy Concern as Influencing Factors for Mobile Protection Behavior

Lydia Kraus, Ina Wechsung, Sebastian Möller
Quality and Usability Lab
Telekom Innovation Laboratories, TU Berlin
Ernst-Reuter-Platz 7, Berlin, Germany
firstname.lastname@telekom.de

ABSTRACT

This paper investigates to which degree privacy and security knowledge and global information privacy concern of a user influence mobile protection behavior. We performed a survey with 154 participants. The results of the survey suggest that both privacy and security knowledge and global information privacy concern are influential for mobile protection behavior. We find that low knowledge and low global information privacy concern can serve as predictors for the non-usage of the evaluated protection methods, whereas high knowledge and high concern can serve as predictors for the usage of the evaluated protection methods.

1. INTRODUCTION

Former work has shown that users lack understanding [1] and awareness [2] of mobile security mechanisms. For instance, Felt et al. [1] found that a large percentage of Android users do not understand the exact meaning of app permissions, which makes it difficult for them to make appropriate security and privacy decisions when downloading mobile applications (apps). Mylonas et al. [2] found in a study among Greek smartphone users that almost half of the users were not aware whether or not apps are tested before being launched in an app repository (such as Google Play for Android or the App Store for iOS). This unawareness might expose especially users who wrongly assume that apps are tested before being launched to privacy or security risks. Also, they found that technology and security savvy users were more likely to pay attention to security messages [2].

However, non-technology savvy users can obtain advice on how to protect their online privacy. For instance, several websites and reports exist with recommendations on how to protect one's mobile privacy [3-6]. Whereas former work on the influence of privacy knowledge concentrated on self-reported knowledge, awareness, and behavior in the context of internet usage and protection against marketing companies [7,8], we measure how well everyday privacy and security (P&S) advice such as provided in [3-6] and P&S concepts are known to users. Therefor we developed a P&S knowledge questionnaire to measure users' knowledge of everyday privacy and security advice and of P&S concepts. Details about the questionnaire can be found in [9].

We envision the P&S knowledge questionnaire as an additional instrument to categorize users of privacy and security applications. Furthermore, it should serve as a tool to assess whether newly developed technologies can be used without obstacles by both knowledgeable and non-knowledgeable users. Therefore, during the development of privacy enhancing technologies or security mechanisms, P&S knowledge could be used in user studies to examine whether all users (and not only those with high knowledge) are able to use the developed technology without obstacles.

We conducted an online survey with 154 participants to test the P&S knowledge questionnaire and to investigate the influence of P&S knowledge and, in addition, global information privacy concern (hereafter referred to as "privacy concern") on mobile protection behavior. The goal of our work is to investigate whether, and to which degree, P&S knowledge and global information privacy concern influence the usage of mobile protection methods.

The results suggest that there is a difference in mobile protection behavior between participants of different P&S knowledge levels as well as between participants of different privacy concern groups. We find that both privacy and security knowledge and privacy concern are influential for mobile protection behavior. We also find that P&S knowledge and privacy concern are not correlated.

The paper is structured as follows. In Section 2, the survey set-up is explained and statistics about demographics of the participants are given. In Section 3, the results are analyzed regarding descriptive statistics, correlations and associations between the variables, and regression. The paper closes with discussion, limitations and future work in section 4.

2. METHODOLOGY

2.1 Online survey set-up

The online study consisted of several parts. The questionnaires for P&S knowledge and global information privacy concern are given in the appendix of this document.

P&S knowledge was measured with a multiple choice test consisting of 11 questions with four suggested solutions each, of which three were wrong and one was correct [9]. In addition, each item included a "don't know" option. Privacy concern was measured with the Global Information Privacy Concern (GIPC) Scale which was used in Malhotra et al. [10] for cross validation of the IUIPC scale. The GIPC scale contains six items on a 7 point scale from 1 = *strongly disagree* to 7 = *strongly agree* [10].

We decided to use this privacy concern questionnaire as we assume the six items to allow for a finer assessment of general privacy concern compared to Westin's index which consists of three statements only [11]. There are other privacy concern scales for instance IUIPC [10] or DPC [12] which might provide an even finer classification of privacy concern. However, using these scales would have resulted in a rather long survey. The survey's focus was mainly on P&S knowledge and thus already contained more than 40 questions excluding privacy concern. A much longer survey, however, might have led to fatigue of respondents and successive low data quality.

The order of the survey parts was as follows:

- Demographics
- Internet usage
- Smartphone usage
- Global Information Privacy Concern [10]
- P&S knowledge questions [9]
- Mobile protection behavior[1]
    - Do you use one or several of the following messaging apps with encrypted data transmission? (Secure messenger apps)
    - Do you use one or several of the following apps to protect you smartphone against threats? (Anti-virus apps)
    - Do you use one or several of the following apps to track your smartphone in case of theft? (Anti-theft apps)
    - Do you use one or several of the following apps to protect your privacy on your smartphone? (Privacy protection apps)
    - Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Refrain – high number of permissions)
    - Did you ever refrain from installing an app due to unusual permissions? (Refrain – unusual permissions)
    - Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Uninstall – privacy intrusiveness)

2.2 Participants

The survey was completed by 154 participants between 18 and 59 years old (M = 29.61, SD = 9.19). They were recruited on an online portal for voluntary study participants hosted by our university. 67 participants (43.2%) were male and 86 (55.5%) were female, 2 (1.3%) did not report their gender. Participants with less than a secondary school degree (15.4%), secondary school degree (43.2%), and university degree (41.3%) were represented; there was a bias towards higher education levels. Various occupational groups were represented with a bias towards students (54.2%). 35 participants (22.7%) had professional IT expertise, whereas 119 participants (77.3%) did not have professional IT expertise. Current and past work in a profession related to IT, computer science, communications engineering, and similar professions were considered IT expertise. Also students of these areas were considered as having professional IT expertise. The majority (N=137, 89%) of participants were smartphone users (Android (N=88, 56.8%), iOS (N=41, 26.5%), "Other" (N=8, 5.8%)).

[1] For the security and privacy apps we gave examples of often downloaded Android and iOS apps with these features. We also gave participants the option "other" to specify if they use other apps with similar features.

3. RESULTS

3.1 Descriptive statistics

A P&S score was calculated by summing the number of correct answered questions of the 11 items scale. Also a mean value for privacy concern was computed based on the answers of the items. Descriptive statistics of the P&S score and privacy concern (PC) score are given in Table 1. The quartiles were used for both, P&S knowledge and privacy concern, to divide participants into categories of low, medium, and high knowledge and concern, respectively.

Table 1. Descriptive statistics: P&S and Privacy Concern (PC) score.

	Min	1st Qu	Mean	Median	3rd Qu	Max
P&S (*N* = 154)	1	6	7.71	8	9	11
PC (*N* = 154)	1	4	4.75	4.83	5.54	7

3.2 Correlations and associations between demographics, P&S knowledge, and privacy concern

3.2.1 Correlations

There was no significant correlation (Pearson product-moment correlation) between P&S knowledge and privacy concern, $r = 0.106$, $N = 154$, $p = 0.190$.

Age and privacy concern show a significant positive correlation, thus the higher the age of the participants, the higher was their privacy concern. This is in line with results of [13] who also found that age has a positive influence on privacy concern. No correlation was found between age and the P&S score. An overview of Pearson correlations between age and the P&S score and between age and the PC score is given in Table 2.

Table 2. Correlations between age, P&S knowledge and PC.

	r	*N*	*p*
Age - P&S	-0.063	154	0.44
Age - PC	0.181*	154	0.025

*Significant on the 0.05 level

3.2.2 Associations

We used χ^2-tests and corresponding phi-coefficients to determine whether there is an association between the categorical demographic variables and P&S knowledge groups as well as privacy concern groups. We tested associations for gender, education, IT expertise, frequency of internet usage, frequency of smartphone usage, and smartphone operating systems. For P&S knowledge we found three significant associations, whereas for privacy concern we did not find any significant association. Table 3 gives an overview of results for P&S knowledge.

Table 3. Associations between categorical demographic variables and P&S categories.

	χ^2	*df*	*p*	*φ*
Gender	21.03	4	.000	.372**
Education	11.78	4	.018	.277*
IT expertise (Y/N)	19.82	2	.000	.359**
Internet usage	3.41	6	.775	.149
Smartphone usage	10.15	10	.431	.272
Smartphone OS	1.48	4	.838	.098

* Significant on the 0.05 level; ** significant on the 0.01 level

There was a significant association between gender and P&S knowledge. Male participants were less likely to have low P&S knowledge whereas female participants were less likely to have high P&S knowledge compared to the complete sample. Also, there was a significant association between participants with different education levels. Participants who had less than a secondary high school degree were more likely to have low P&S knowledge and less likely to have high P&S knowledge compared to the complete sample. Also, IT expertise showed to have a significant association with P&S knowledge. Participants without IT expertise were more likely to have low and medium P&S knowledge, whereas participants with IT expertise were less like to have low or medium P&S knowledge compared to the complete sample.

Table 4 gives an overview of results for privacy concern. Our results regarding the effect of gender and internet usage on privacy concern are similar to [13]. Zukoswki and Irwin [13] did not find an effect of gender on privacy concern and of internet experience on privacy concern. In contrast to [13], we did not find an effect of education level on privacy concern.

Table 4. Associations between categorical demographic variables and privacy concern.

	χ^2	*df*	*p*	*φ*
Gender	1.68	4	.886	.105
Education	3.08	4	.556	.141
IT expertise (Y/N)	0.40	2	.841	.051
Internet usage	9.47	6	.142	.248
Smartphone usage	12.64	10	.227	.304
Smartphone OS	1.35	4	.851	.094

3.3 Differences in mobile protection behavior

Figure 1 shows the percentage of users applying a specific protection behavior. For all protection behaviors except "private browsing" only smartphone users were considered.

Pearson χ^2-tests were computed to investigate the relation between P&S knowledge and mobile protection behavior as well as between privacy concern and mobile protection behavior (cf. Table 5).

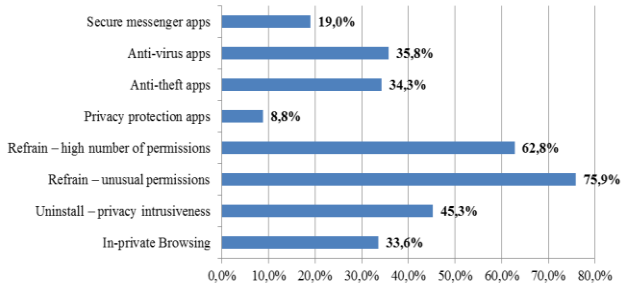

Figure 1. Percentages of people indicating to apply a specific behavior.

As shown in Table 5, in all considered cases with significant differences between the P&S knowledge groups, participants with high knowledge were more likely to report mobile protection behavior. For the usage of secure messenger apps participants with low P&S knowledge were less likely to use these kinds of apps. Regarding the uninstalling of privacy-intrusive apps participants with medium P&S knowledge also were less likely to report the behavior.

For privacy concern, in all considered cases with significant differences between the privacy concern groups, participants with low concern were less likely to report mobile protection behavior. Only for the uninstalling of privacy-intrusive apps, participants with high privacy concern were more likely to report this behavior.

Table 5. Differences in behavior between different groups of P&S knowledge and privacy concern[a].

Behavior	P&S	PC
1. Do you use messenger apps with encrypted transmission? (Yes[b] = 19%)	**high ↑; low ↓** $\chi^2(2, N=137) = 10.37$; $p=0.005$	**low ↓** $\chi^2(2, N=137) = 6.62$; $p=0.041$
2. Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Yes[b]: 62.8%)	**high ↑** $\chi^2(2, N=135) = 7.23$; $p=0.027$	**low ↓** $\chi^2(2, N=135) = 6.04$; $p=0.041$
3. Did you ever refrain from installing an app due to unusual permissions? (Yes[b]: 75.9%)	-	**low ↓** $\chi^2(2, N=135) = 13.94$; $p=0.001$
4. Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Yes[b]: 45.3%)	**high ↑; medium ↓** $\chi^2(2, N=135) = 7.83$; $p=0.021$	**high ↑; low ↓** $\chi^2(2, N=135) = 12.04$; $p=0.002$
5. Do you use the private browsing function of your browser? (Yes[c]: 33.6%)	**high ↑** $\chi^2(2, N=154) = 10.56$; $p=0.005$	-

[a] For cases 1-4 only smartphone users were considered. "low", "medium" and "high" indicate the P&S knowledge or privacy concern group. Groups and behaviors without significant differences are not reported. The arrows indicate whether a group was either more likely to report a specific behavior (↑) or less likely (↓) compared to the complete sample (post-hoc tests with Bonferroni-correction).
[b] Refers to all smartphone users in the sample.
[c] Refers to the complete sample

3.4 Regression analysis

We performed several binary logistic regression analyses to further explore the suitability of privacy concern and P&S knowledge as predictors for mobile protection behavior. For each logistic regression one of the behaviors reported in Table 5 was the outcome (dependent) variable. The outcome variable was either coded as "0" (no), i.e. a specific behavior is not reported, or "1" (yes), i.e. a specific behavior is reported.

Binary logistic regression can be used for dichotomous outcome variables as it predicts the probability that a certain case either falls into category "0" (i.e. a specific behavior is not reported) or "1" (i.e. a specific behavior is reported) [14]. Thereby, the *B*-value indicates the logistic regression coefficient whereas the *Exp(B)* value indicates the odds ratio. The odds are the ratio of the probability that an event occurs ("1") to the probability that an event does not occur ("0") [14]. For a categorical variable, the odds ratio is the ratio of the odds of one category to the odds of the reference category.

In contrast to linear regression, for binary logistic regression there does not exist a linear measure of effect size (R^2). R^2 is the proportion of variance that is explained by the model. Thus, the higher the R^2, the better is the model fit. However, for logistic regression, several pseudo-R^2 measures exist such as Hosmer & Lemeshow's measure (the formula to calculate this measure is the same as for McFadden's measure), Cox & Snell's measure, and Nagelkerke's measure [14]. Suggestions on how to interpret R^2 in binary logistic regression are given in Erichson et al. [15]: R^2 values (McFadden/ Hosmer & Lemeshow/ Cox & Snell) higher than 0.2 can be considered as acceptable, whereas R^2 values higher than 0.4 can be considered as good model fit. For Nagelkerke's R^2, values larger than 0.2 can be considered as acceptable, larger than 0.4 as good and 0.5 as very good model fit.

Another statistic for interpreting the results of logistic regression is the model χ^2 statistic. If the model χ^2 statistic is significant, the model predicts the outcome significantly better than the baseline model [14]. Thereby, the baseline model refers to the model that contains only the constant term without any other predictors.

Our analysis is of explorative nature and we also included other factors that might influence the behavior such as smartphone OS, IT expertise, or age. We selected the forced entry method where all possible predictors are fed into the model simultaneously. Predictors for which the Wald statistic was significant were included in the model. If the Wald statistic is significant it means that the predictor has a significant influence on the outcome variable [14]. For all behaviors except "private browsing" we fed the following predictors into the models:

- P&S knowledge: "low" and "medium" were coded in dummy variables and "high" was used as a reference variable
- Privacy concern (PC): "low" and "medium" were coded in dummy variables and "high" was used as a reference variable
- Age
- IT expertise (Y/N)
- Smartphone OS: Android and "other" were coded in dummy variables and iOS was used as a reference variable.

In the following only predictors that had a significant influence on the outcome variable are reported.

3.4.1 Messenger apps with encrypted transmission

The results show that low P&S knowledge and low privacy concern are significant predictors for the usage of secure messaging apps (cf. Table 6). The odds of using secure messaging apps for participants with low P&S knowledge are 0.11 times lower than for participants with high P&S knowledge. The odds of using secure messaging apps for participants with low privacy concern are 0.08 times lower than for participants with high privacy concern. The model predicted 80.3% of cases of the outcome variable correctly.

Table 6. Results of the logistic regression for secure messenger apps as the outcome variable.

Secure messenger apps				95% CI for odds ratio	
Predictor	**B (SE)**	**p**	**Exp(B)**	**Lower**	**Upper**
P&S (low)	-2.24 (.82)	.008	.11	.02	.56
PC (low)	-2.59 (1.16)	.026	.08	.01	.73

R^2 = .16 (Hosmer & Lemeshow), .14 (Cox & Snell), .23 (Nagelkerke). Model χ^2 = 21.16, p<0.01

3.4.2 Refraining from installing an app due to a high number of permissions

The results show that low and medium P&S knowledge as well as low privacy concern and the smartphone OS are significant predictors for refraining from installing due to a high number of permissions (cf. Table 7).

Table 7. Results of the logistic regression for "refraining from installing due to a high number of permissions" as the outcome variable.

High number of permissions				95% CI for odds ratio	
Predictor	**B (SE)**	**p**	**Exp(B)**	**Lower**	**Upper**
Constant	2.26 (1.01)	.026	9.53	-	-
P&S (low)	-1.42 (.64)	.027	.24	.07	.85
P&S (medium)	-1.26 (.62)	.040	.28	.09	.94
PC (low)	-1.27 (.60)	.035	.28	.07	.92
OS (Android)	1.17 (.44)	.007	3.23	1.37	7.64

R^2 = .13 (Hosmer & Lemeshow), .16 (Cox & Snell), .22 (Nagelkerke). Model χ^2 = 23.30, p<0.01

The odds of showing this behavior with low P&S knowledge are 0.24 times lower than for participants with high P&S knowledge. Also, for participants with medium P&S knowledge, the odds are 0.28 times lower than for participants with high P&S knowledge. The odds of showing this behavior with low privacy concern are 0.28 times lower than for participants with high privacy concern. The odds of Android users to report this behavior are 3.23 times higher than for iOS users, which is plausible as iOS users do not see the permissions at the time of installation. The model predicted 63.7% of cases of the outcome variable correctly.

3.4.3 Refraining from installing an app due to unusual permissions

The results show that low privacy concern and smartphone OS are significant predictors for refraining from installing due to unusual permissions (cf. Table 8).

The odds of showing this behavior with low privacy concern are 0.12 times lower than for participants with high privacy concern. The odds to report this behavior are 3.21 times higher for Android users compared to iOS users. This might be as described in Section 3.4.2 due to the fact that iOS users do not see the permissions at the time of installation. The model predicted 80.7% of cases of the outcome variable correctly.

Table 8. Results of the logistic regression for "refraining from installing due to unusual permissions" as the outcome variable.

Unusual permissions				95% CI for odds ratio	
Predictor	**B (SE)**	**p**	**Exp(B)**	**Lower**	**Upper**
PC (low)	-2.16 (.71)	.002	.12	.03	.47
OS (Android)	1.17	.016	3.21	1.24	8.33

R^2 = .15 (Hosmer & Lemeshow), .14 (Cox & Snell), .22 (Nagelkerke). Model χ^2 = 21.03, p<0.01

3.4.4 Uninstalling of privacy-intrusive apps

The results show that low and medium privacy concern, medium P&S knowledge as well as using another smartphone OS than Android and iOS are significant predictors for uninstalling privacy-intrusive apps (cf. Table 9).

Table 9. Results of the logistic regression for "uninstalling of privacy-intrusive apps" as the outcome variable.

Uninstalling of privacy-intrusive apps				95% CI for odds ratio	
Predictor	**B (SE)**	**p**	**Exp(B)**	**Lower**	**Upper**
Constant	2.34 (1.03)	.023	10.41	-	-
P&S (medium)	-1.55 (.57)	.007	.21	.07	.65
PC (low)	-2.08 (.66)	.001	.12	.03	.45
PC (medium)	-1.23 (.50)	.013	.29	.11	.77
OS (other)	-2.57 (1.18)	.030	.08	.01	.78

R^2 = .16 (Hosmer & Lemeshow), .20 (Cox & Snell), .27 (Nagelkerke). Model χ^2 = 30.63, p<0.01

The odds of showing this behavior with low privacy concern are 0.12 times lower and for medium privacy concern they are 0.29 times lower than for participants with high privacy concern. Also the odds of showing the behavior for medium P&S knowledge are 0.21 times lower compared to high P&S knowledge. The usage of "other" smartphone operating systems decreases the odds times 0.08. The model predicted 70.4% of cases of the outcome variable correctly.

3.4.5 Private Browsing

For the logistic regression of the private browsing usage we fed the following predictors into the model:

- P&S knowledge, coded as dummy variable for low and medium and high as a reference variable
- Privacy concern (PC), coded as dummy variable for low and medium and high as a reference variable
- Age
- IT expertise (Y/N)
- Browser usage (categorical, coded in dummy variable for Google Chrome, Mozilla Firefox, Internet Explorer, Opera and other, Safari as reference category)
- Smartphone usage (we distinguished here between smartphone users and no smartphone users)

The results of the analysis are given in Table 10. The overall p-Value of the model showed not to be significant (p=.20). Thus, we will not interpret the model in detail.

Table 10. Results of the logistic regression for "private browsing" as the outcome variable.

Private Browsing				95% CI for odds ratio	
Predictor	**B (SE)**	**p**	**Exp(B)**	**Lower**	**Upper**
P&S (low)	-1.45 (.54)	.007	.23	.08	.67
P&S (medium)	-1.24 (.49)	.012	.29	.11	.76

R^2 = 0.08 (Hosmer & Lemeshow), .10 (Cox & Snell), .13 (Nagelkerke). Model χ^2 = 15.66, p=0.20

4. DISCUSSION, LIMITATIONS AND FUTURE WORK

We conducted an online study with 154 participants to investigate whether and to which degree P&S knowledge and global information privacy concern influence the usage of mobile protection methods.

Both, the results from the χ^2-tests and the logistic regression analyses suggest that P&S knowledge and privacy concern are influential on mobile protection behavior.

In the regression analyses, all models (except the model for usage of private browsing) showed significant improvement when either P&S knowledge or privacy concern or both were added as predictors.

The odds ratios for both P&S knowledge and privacy concern range between 0.08 and 0.29. This suggests that there is a strong association with the outcome variable[2]. Also, P&S knowledge and privacy concern show within most behaviors similar odds ratios, which indicates that their strength of influence on the outcome variable is similar.

For the usage of secure messenger apps, P&S knowledge and privacy concern had the lowest odds ratios compared to the other behaviors. Thus, the active decision for installing a protection

[2] We interpreted this according to Wang [16] who suggests interpreting odds ratios of larger than 3 as strong associations with the outcome variable. As the odds ratios in our case are smaller than 1 we conclude that an odds ratio of 1/3 is to be interpreted similar than an odds ratio of 3, however, with different effect direction.

method on a device might be influenced the strongest by these two independent variables.

The R^2 values of the significant models were similar and ranged between 0.13 and 0.2 (Hosmer & Lemeshow, Cox & Snell) and 0.22 and 0.27 (Nagelkerke). When interpreting Nagelkerke's R^2 the model fit is acceptable, whereas interpreting Hosmer & Lemeshow and Cox & Snell suggests a limited model fit.

For some behaviors, namely "refraining from app installation due to unusual permissions" and "private browsing", either P&S knowledge or privacy concern were influential. This may indicate that mobile protection behaviors for which P&S knowledge is not a significant predictor are easier applicable by people without P&S knowledge. For example users could be educated by the media about unusual permissions [17].

As P&S knowledge and privacy concern are not correlated, we suggest to use P&S knowledge as an additional factor besides privacy concern to segment users of privacy and security applications. Also, in contrast to concern, P&S knowledge can be influenced by educating users and giving them concrete advice on how to protect their devices.

So far, we did not cover all possible protection behaviors and we plan in future studies to ask users about more kinds of protection behaviors, such as the usage of phone encryption or the scrutinizing of permissions before installing an app (mainly applies to Android users). Also, we would like to cluster the behaviors in categories.

In future studies, we would also like to investigate whether mobile protection behavior could be better predicted if privacy concern is measured with a mobile information privacy concern instrument. A scale for mobile users' information privacy concern was for instance developed in [18].

The P&S questionnaire is still under development and some items need to be adjusted. Also, the smartphone OS showed to be a significant predictor for refraining from installing due to a high number of permissions or to unusual permissions, and for uninstalling privacy-intrusive apps. As iOS users do not see the permissions at the time of installation it would have been better to formulate these items differently. In general, risks might be perceived differently by iOS and Android users [19], which might either be due to the operation system itself (as for the permissions) or to differences between the user groups in terms of user characteristics (e.g. personality factors) .

As our sample was biased towards higher education levels and students, generalizations about the results should be made with caution. Therefor we plan to conduct further studies with a more diverse sample.

5. ACKNOWLEDGMENTS

This work has been supported by the EU FP-7 support action ATTPS under grant agreement no. 317665. We would like to thank Jens Ahrens and Josh Sorenson for proofreading the paper. Furthermore, we would like to thank the anonymous reviewers for their helpful comments.

6. REFERENCES

[1] Porter Felt, A.; Ha, E.; Egelmann, S.; Haney, A.; Chin, E. & Wagner, D.: Android Permissions: User Attention, Comprehension, and Behavior, *Symposium on Usable Privacy and Security*, Washington, DC, USA, 2012

[2] Mylonas A.; Kastania A.; Gritzalis D.: Delegate the Smartphone user? Security awareness in smartphone platforms. *Computers and Security*, 34, 47-66, 2013

[3] Data Privacy Day - http://www.staysafeonline.org/data-privacy-day/privacy-tips/mobile

[4] Hogben, G.,; Dekker, M.: Smartphones: Information security risks, opportunities and recommendations for users, *ENISA European Network and Information Security Agency*, 2010

[5] Microsoft Safety and Security Center: 4 safety tips for using Wi-Fi, http://www.microsoft.com/en-gb/security/online-privacy/public-wireless.aspx

[6] Consumer Action: How to Make Smart Wireless Choices and Avoid Problems: http://www.consumer-action.org/english/articles/cell_phone_savvy_training_manual/#protect-info

[7] Park, Y. J.: "Digital literacy and privacy behavior online." *Communication Research* 40.2, 215-236, 2013

[8] Youn, S.: "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents." *Journal of Consumer Affairs* 43.3, 389-418., 2009

[9] Kraus L.; Hirsch T.; Wechsung I.; Poikela M.; Möller S.: Poster: Towards an Instrument to Measure Everyday Privacy and Security Knowledge. Unpublished, accepted for publication at the *Symposium on Usable Privacy and Security (SOUPS)*, Menlo Park, CA, USA, 2014

[10] Malhotra, N. K.; Kim, S. S. & Agarwal, J.: Internet Users' Information Privacy Concern (IUIPC): The Construct, the Scale and a Causal Model. *Information Systems Research*, 15, 336-355, 2004

[11] Kumaraguru P., Cranor L.F.: A Survey of Westin's Studies. *Institute for Software Research International*, 2005

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

[13] Zukowski, T., Irwin, B.: Examining the influence of demographic factors on internet users' information privacy concerns, *Annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. ACM, 2007

[14] Field, A.: Discovering Statistics using SPSS, Sage publications, 2009

[15] Erichson, B., Plinke W., Weiber, R.: Multivariate Analysemethoden. Ed. Klaus Backhaus. Vol. 11. Berlin: Springer, 2006.

[16] Wang, F.-L.: Logistic Regression: Use & Interpretation of Odds Ratio (OR); available online: http://www.sas.com/offices/NA/canada/downloads/presentations/CSUG-Oct2011/Wang-Logistic-Regression.pdf

[17] http://www.businessnewsdaily.com/3768-smartphones-apps-share-personal-data.html

[18] Xu, Heng, et al. "Measuring Mobile Users' Concerns for Information Privacy." *ICIS*. 2012.

[19] Benenson Z., Reinfelder, L.: Should the Users be Informed? On Differences in Risk Perception between Android and iPhone Users. *Workshop on Risk Perception in IT Security and Privacy, Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, 2013

7. APPENDIX

Classification tables of the regression analyses:

Table 11. Secure messenger apps.

Predicted/ Observed	No	Yes	Percentage correct
No	108	3	97.3%
Yes	24	2	7.7%
Overall percentage			80.3%

Table 12. Refraining due to a high number of permissions.

Predicted/ Observed	No	Yes	Percentage correct
No	22	27	44.9%
Yes	22	64	74.4%
Overall percentage			63.7%

Table 13. Refraining due to unusual permissions.

Predicted/ Observed	No	Yes	Percentage correct
No	8	23	25.8%
Yes	3	101	97.1%
Overall percentage			80.7%

Table 14. Uninstalling of privacy-intrusive apps.

Predicted/ Observed	No	Yes	Percentage correct
No	58	15	79.5%
Yes	25	37	59.7%
Overall percentage			70.4%

Table 15. Private browsing.

Predicted/ Observed	No	Yes	Percentage correct
No	92	11	89.3 %
Yes	35	16	31.4 %
Overall percentage			70.1 %

The questionnaires used in the study were the following:

Global Information Privacy Concern Scale [10]
(The first item was slightly modified compared to [10])

- All things considered, the Internet causes serious privacy problems.
- Compared to others, I am more sensitive about the way online companies handle my personal information.
- To me, it is very important to keep my privacy intact from online companies.
- I believe other people are too much concerned with online privacy issues. (reversed)
- Compared with other subjects on my mind, personal privacy is very important.
- I am concerned about threats to my personal privacy today.

P&S knowledge [9]

In the following, answer "A" is always correct, but during the survey the answer order was randomized.

- **How can a user protect herself against data abuse while surfing in a public network?** (M = .82, SD = 39; A: Avoid entering sensitive data on websites, B: Store the network password on the device, C: Delete the browser history after surfing, D: Disable location-based services on the device)
- **How can a device be protected from viruses?** (M = .82, SD = .38, A: Always keep software and OS up-to-date, B: Don't enter personal data on websites, C: Avoid using wireless networks, D: Only visit websites that were recommended by friends)
- **How can a smartphone be protected from malicious apps?** (M = 0.84, SD = .36, A: Only install apps from trustworthy sources, B: Check if the downloaded app provides legal info, C: Try to use apps only occasionally, D: Check if the app publisher has a website)
- **When using an online-banking app: how can the user protect herself against threats?** (M = 0.67, SD = .47, A: Secure the app with an additional password; B: Banking apps are always secure and don't need additional security means, C: Only use the app in urgent cases, D: Increase the security by modifying the source code of the app.)
- **What is the goal of encrypted data transmission?** (M = .61, SD = .49, A: The data can't be eavesdropped, B: The data is protected against viruses, C: The data can't be lost during transmission, D: Only the user herself can see the data)
- **What is malware?** (M = .83, SD = .38, A: Software which is unwanted and might be harmful, B: Software which is not working properly, C: Software which is automatically updating itself, D: A faulty technical device)
- **What is phishing?** (M = .77, SD = .43, A: The interception of personal information via faked routes, B: The analysis of user's browsing behavior C: The sending of unwanted ads, D: The uninstalling of software that needs too much resources)
- **What is social engineering*?** (M = .26, SD = .44, A: To spy out somebody's personal environment online

with the goal to use this information to undertake criminal activities such as identity theft or fraud B: To distribute software-testing tasks to several engineers in order to find security leaks, C: The development of software for social networks, D: The development of charitable apps which are free of charge) *Note: this item should be changed to "What is a social engineering technique?"

- **What is controlled by privacy settings in social networks?** (M = .84, SD = .36, A: The personal information that is shared with other people or apps, B: The personal information that can be seen by the provider of the network, C: The user data which is forwarded to other social networks, D: The user data which can be stored by the provider of the network)
- **What are web analytics?** (M = .66, SD = .47, A: Software which analyzes the behavior of website visitors, B: Software used by search engines to sort results by relevance, C: Software which automatically interlinks text on websites, D: Software, which analyzes HTML code for efficiency)
- **What is written in a privacy policy?** (M = .58, SD = .50, A: If and how a company processes personal information, B: What the user has to do in order to protect her data, C: How private data is classified in general, D: That personal information is always processed in anonymized form)