Factors of Intention to Use a Photo Tool: Comparison between Privacy-enhancing and Non-privacy-enhancing Tools

Vanessa Bracamonte[1], Sebastian Pape[2], and Sascha Löbner[2]

[1] KDDI Research, Inc., Japan va-bracamonte@kddi-research.jp
[2] Goethe University Frankfurt, Germany
{sebastian.pape,sascha.loebner}@m-chair.de

Abstract. Tools that detect and transform privacy sensitive information in user content have been proposed to enhance privacy in contexts such as social media. However, previous research has found that privacy-related concerns can be higher in these types of tools compared to similar non-privacy tools. In this paper, we focus on adoption of these tools and investigate how the knowledge that a data-processing tool has a privacy purpose affects privacy-related factors of intention to use such a tool, when compared with a similar tool with a non-privacy-related purpose. We conducted a user study where we described a privacy-enhancing and a non-privacy-enhancing photo manipulation app to two groups of participants. The results show that general and context-specific privacy-related perception has different effects for the two types of apps. In particular, although participants perceived the same level of privacy risk towards both types of apps, this risk only had a significant negative effect on intention to use in the case of the privacy-enhancing app. Furthermore, disposition to value privacy increased both perceived risk and intention to use the privacy-enhancing app. We discuss these findings in the context of the diffusion of privacy-enhancing tools for user content.

Keywords: Privacy-enhancing tools · Privacy · Risk · User perception

1 Introduction

Users increasingly reveal great amounts of personal information, related to themselves or others, on social media. The consequences of sharing this information can be negative and result in regret from users [32, 28]. Automated analysis of images has been proposed as a way of protecting peoples' privacy in a social media context [20]. In general terms, these proposals work by analyzing the content of peoples photos to detect whether the content reveals private or sensitive information and potentially transforming that content to anonymize it [21, 12]. However, research on perception towards privacy tools has identified that users have privacy-related concerns towards these types of tools. In the evaluation of third-party tracking blockers, Schaub et al. [27] reported that some participants distrusted the tools because of the perception that the tools themselves would

collect their personal data, even though the trackers could do the same. In a study on privacy add-ons, Corner et al. [3] also found that some users distrusted the tools because they thought the tool itself would be used to access their data. Although people understand and agree with the beneficial purposes of a privacy-enhancing tool that analyses their data, they also worry about surveillance and having their privacy intruded upon by these tools [2, 1]. In principle, there is not much to distinguish a privacy-enhancing tool and a non-privacy enhancing tool besides the purpose of protecting privacy. For both types of tools, users would have to provide their photos in order to receive the service. However, previous research has found that for privacy-enhancing tools that process user content, the level of privacy concern can be higher than for similar tools with a non-privacy related purpose [1].

Although there is evidence of a different level of privacy-related concern towards privacy-enhancing tools, research has not examined whether this difference also applies to the mechanism of intention to adopt such a tool. The objective of this study is to investigate if the perception towards privacy-enhancing tools might be different from tools that process data for a non-privacy-related purpose. We conducted a user experiment to examine how the knowledge of the privacy-enhancing purpose of the tool influenced the effect of privacy-related factors on intention to use the tool, compared to a non-privacy-enhancing tool. The results indicate that there is a difference in the relationship between factors for these two types of tools. In particular, risk perception negatively influences the intention to use the privacy-enhancing app, but does not significantly affect the non-privacy-enhancing app. In addition, for the privacy-enhancing app, disposition to value privacy had a significant positive influence on intention to use the app, but for the non-privacy-enhancing app, there is no significant effect. The contribution of this research is a clarification of the mechanism through which privacy-related factors have contrary effects on intention to use a privacy-enhancing tool.

2 Methodology

In this section we describe the methodology used for the study, including the research questions, experiment design and ethical considerations.

2.1 Research Objectives

The study focuses on examining any differences in user perception towards a privacy-enhancing and non-privacy-enhancing tool, in light of the fact that both types of apps have the same potential for privacy risk. In order to do so, we use a privacy-focused model of intention to use a technology, adapted from [23, 6]. The research model is presented in Figure 1. The model establishes that context-specific privacy-related constructs (Perceived risk, Perceived benefit and Trust) influence Intention to use the tool. In addition, it also establishes that privacy-related dispositions and experience (Disposition to value privacy and Prior privacy experience) influence all context-specific constructs. The relationships

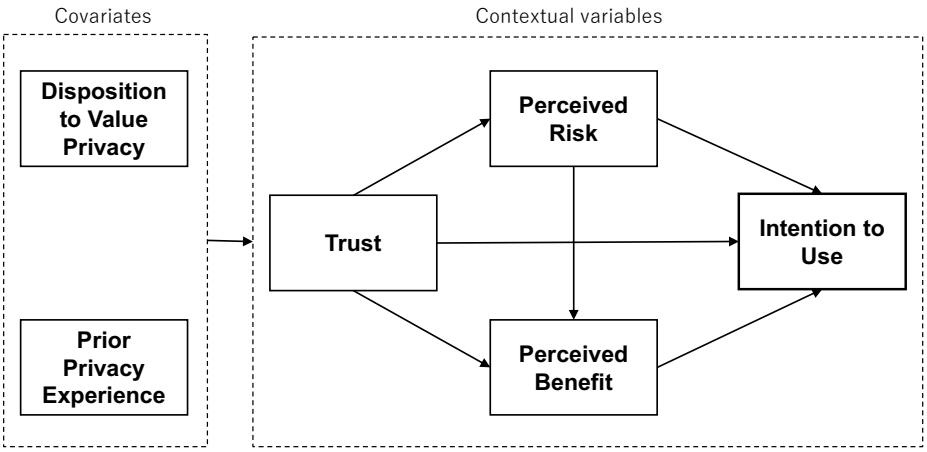

Fig. 1. Research model.

between the constructs in the model have been proposed and validated in previous research [23, 6, 5]. As mentioned, the focus in this study is in the differences that may arise due to the type of tool priming. More specifically, we seek to answer the following questions:

- Are there differences in the relationships between privacy-related factors and intention to use for privacy-enhancing and non-privacy-enhancing tools?

- Are there differences in the relationships between general privacy attitudes and experiences, and privacy-related factors of intention to use, for privacy-enhancing and non-privacy-enhancing tools?

2.2 Experiment Design and Task

In order to answer the research questions, we designed an experiment which consisted of a task for participants to read and give their opinion about an hypothetical app that would be used to transform photos for uploading on social media. We manipulated the purpose of app: privacy-enhancing vs. non-privacy-enhancing. The objective of this study was to evaluate differences in perception that resulted from the manipulation (priming), therefore, the privacy-enhancing app was explicitly described as such. Participants viewed the description and a mockup of only one type of app (between-subjects design). After reading about the app, the participants answered a questionnaire.

We described to participants an hypothetical free, third-party app for social media photos. For the privacy-enhancing app, the purpose was described as protecting privacy; for the non-privacy-enhancing app, the purpose was described as enhancing the content for fun. The app would hypothetically work by analyzing and detecting the content in the users' photos. We described the type of information the app would detect from the photos: private information for the

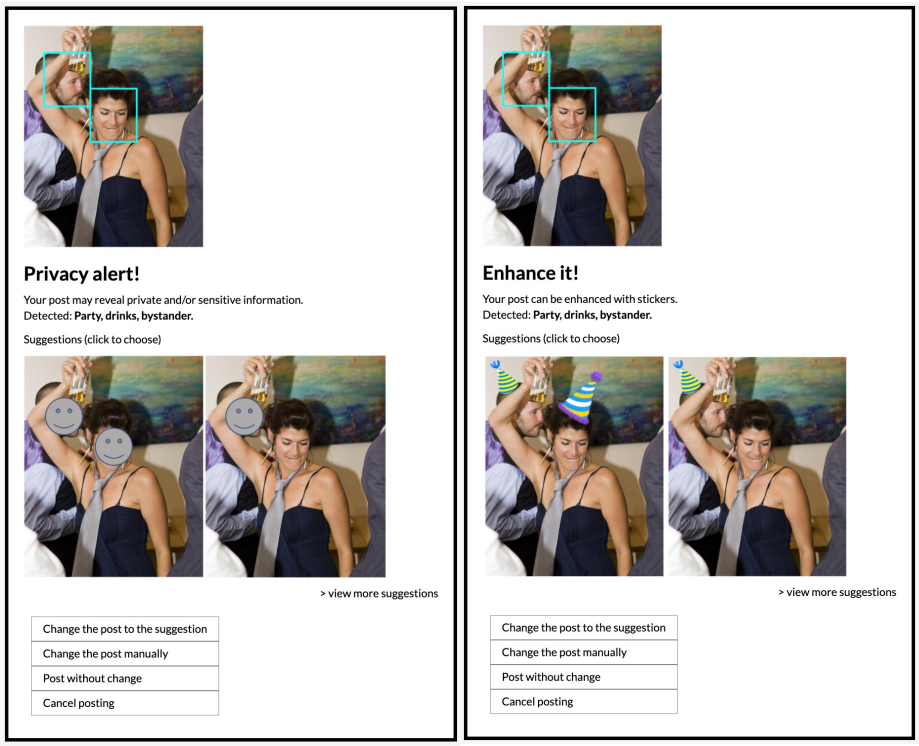

Fig. 2. Experiment app mockups. Left: Privacy-enhancing app. Right: Non-privacy-enhancing app.

privacy-enhancing app, and information that could be enhanced with stickers for the non-privacy-enhancing app. We then presented a non-interactive mockup of the app which showed how it would work. The mockups for each group had the same general design, and only differed in their message and the transformation performed on the photo (privacy-enhancing vs non-privacy enhancing) The detail of the app mockup is shown in Figure 2. After the mockup, we showed five additional photo examples to the participants. Photos were sourced from the COCO dataset [22].

We measured the constructs of interest with scales adapted from previous research: Intention to use [24], Perceived benefit [6], Perceived risk [23], Trust [15], Disposition to value privacy [33] and Prior privacy experience [29]. The responses used a 7-point scale, ranging from *Strongly disagree* to *Strongly agree*, except for Prior privacy experience which was measured on a 7-point scale, ranging from *Never* to *Very frequently*. The detail of the measurement items is shown on Table 1. The questionnaire also included age, gender (as an open text box [30]), frequency of social media posting and attention check questions.

We validated the questionnaire with pretests conducted with Amazon Mechanical Turk workers. The pretest workers were compensated with US$1.7 and we rewarded an additional US$1 to participants who provided detailed feedback. In the pretests, we also validated that it was clear to the participants what was the purpose of the app (privacy-related or non-privacy-related).

Table 1. Measurement items

Intention to use	Given the chance, I intend to use this app. Given the chance, I predict that I would use this app in the future. It is likely that I would use with this app in the future.
Perceived risk	In general, it would be risky to give my photos to this app. In general, it would be risky to give personal information to this app. There would be high potential for privacy loss associated with giving personal information to this app There would be too much uncertainty associated with giving personal information to this app. Providing this app with personal information would involve many unexpected problems. (reverse scale)
Perceived benefit	Revealing my personal information on this app will help me obtain the result I want. I need to provide my personal information so I can get exactly what I want from this app. I believe that as a result of my personal information disclosure, I will benefit from a better, customized result.
Trust	I would feel safe giving personal information to this app. This app would tell the truth and fulfill promises related to the information provided by me. I trust that this app would keep my best interests in mind when dealing with my personal information.
Disposition to value privacy	Compared to others, I am more sensitive about the way my personal information is handled. Keeping my information private is the most important thing to me. Compared to others, I tend to be more concerned about threats to my information privacy.
Prior privacy experience	How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce web site without your authorization? How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet? How often have you personally been the victim of what you felt was an improper invasion of privacy?

2.3 Participant Recruitment and Ethical Considerations

We recruited participants on Amazon Mechanical Turk with the following qualifications: workers from the USA, who had at least a 99% acceptance rate for their tasks, and who had worked on at least 5000 tasks. We set the participant reward at US$2.5 (US$11.5/hour rate for a 11 minute survey). We obtained 400 responses in total and we identified 20 responses which were duplicated submissions or had answered the attention questions with unrelated content. These responses were rejected and the rest of participants (380) were rewarded.

This study was exempt from review according to our institution's criteria for research of this type. Nevertheless, we provided a notice to inform potential participants about the characteristics of the study. The notice included a description of the purpose of the survey, the approximate time to finish it and the task participants were expected to do (read a description and answer questions). The notice also explained that the survey included attention questions, but that we would not reject the participants answers based only on these questions. However, we clarified that we would reject duplicated answers or answers unrelated to the question asked. We indicated that the survey was completely voluntary and that participants were free to decline to participate, that we would not collect identifying information such as name, email or IP address, and that the results would be used for academic purposes only. We also indicated that the survey was limited to adults who lived in the United States. Finally we provided the principal researchers' name and email address in case of any questions about the study. Participants were asked to access the link to the survey itself if they accepted to participate.

3 Results

In this section, we describe the sample obtained and the results of the data analysis.

3.1 Sample

We first identified 22 multivariate outliers using the Mahalanobis distance (alpha = 0.001). We removed these cases from analysis, resulting in a sample size of 358 participants (exactly 179 in each group). This sample size is over the minimum sample required for finding path coefficients of 0.11 - 0.2, with a significance level of 5% and a power of 80% [7], based on the inverse square root method for minimum sample size estimation [18]. The age mean was 41 for both groups, with a median of 37 years-old in the Privacy app group and 38 years-old in the Non-privacy app group. The gender distribution was 93 (52%) female / 86 (48%) male participants in the Privacy app group and 101 (56%) female / 78 (44%) male participants in the Non-privacy app group.

We compared the characteristics of participants between groups using non-parametrical tests. Mann-Whitney U tests indicated that there were no significant

differences in age ($p = 0.94$), gender ($p = 0.4$) or frequency of social media posting ($p = 0.11$) between groups. The sample results indicate that the participant groups are comparable.

3.2 Group Comparison

We used a partial least squares structural equation modeling (PLS-SEM) method to evaluate the hypotheses of the study. This method accounts for interrelationships between the constructs of interest and for data which may not be normally distributed [8]. We conducted the PLS-SEM analyses using SmartPLS (v.3.3.9) [25]. The focus of this study is to investigate differences between the experiment groups. In other words, we evaluate if participant perception is influenced by the privacy purpose priming. In order to do this, we conducted a PLS-SEM analysis, in particular, a multigroup analysis (PLS-MGA [13]).

First, we evaluated the reliability and validity of the measurement model. We examined indicator reliability by inspecting the items loading on their respective constructs, that is, the correlation weights between the construct and its indicators (measurement items). All loadings had a value over the threshold of 0.708 [8], ranging from 0.821 to 0.992. To evaluate internal consistency reliability, which is the association between indicators of the same construct, we examined the rhoA reliability coefficient [4]. For all constructs, rhoA values were higher than the satisfactory minimum of 0.7 [7], ranging from 0.836 to 0.99. The rhoA values were higher than the ideal upper limit of 0.9, but this was likely due to the use of established scales from previous research. Convergent validity, which is how much the construct converges to explain indicator variance, was examined using the average variance extracted (AVE). The AVE for all constructs had a value above the minimum level of 0.5 [8], ranging from 0.74 to 0.981. We examined discriminant validity, which is how much a construct is distinct from other constructs, using the heterotrait–monotrait (HTMT) ratio of correlations criterion. As required, all values were significantly lower than the threshold value of 0.9 [7], ranging from 0.04 to 0.775.

Before the multigroup comparison analysis, we conducted a measurement invariance of composite models (MICOM) procedure [14] to validate that the models can be compared. The procedure consists of three steps to test for configural invariance, compositional invariance, and composite mean values and variances equality. The first two steps are necessary to establish partial measure invariance, which is required to be able to meaningfully compare the structural model between groups. The first configural invariance step requires that the data has the same handling, that all constructs have the same measurement items, and the same estimation settings are used across groups. We ensured that these requirements were met for our analysis. The second compositional invariance step requires that the constructs are formed equally in the groups. We conducted a permutation test to evaluate compositional invariance. The results show that no correlations were significantly different ($p > 0.05$) and all fall within the 95% confidence interval, which indicates compositional invariance of the models for all constructs. We then tested the composite mean values and variances equality.

The results show that Intention to use (difference in mean = 0.229, p=0.033) and Perceived benefit (difference in mean = 0.332, p=0.002) were significantly different between groups in terms of composite mean value. All other constructs had equal mean values and variances. The positive difference in mean indicates that Intention to use and Perceived benefit were significantly higher for the privacy app. Although this is not the focus of the analysis, we interpret this result to simply reflect a difference in the benefit of the hypothetical apps, of enhancing privacy in comparison to enhancing enjoyment.

The results of the MICOM procedure indicate that there was partial measurement invariance, due to the significant differences in the mean of Intention to use and Perceived benefit. Therefore we also examined the difference in structural models in terms of the standardized path coefficients between groups. We first validated the quality of the structural models, by examining collinearity issues and the coefficient of determination (R-squared). Collinearity (too high correlation) issues in the structural models was examined by calculating the variance inflation factor (VIF) values for the constructs. All VIF values were below 5, that is, below threshold for critical collinearity [8]. The values ranged from 1.111 to 3.373. R-squared values measure the variance in a construct explained by the predictors; values of 0.25 are considered weak [8]. The values ranged from 0.1 to 0.704. Trust was the only construct with a value lower than 0.25 (0.1 in the Privacy app group and 0.163 in the Non-privacy group), but this was due the covariates being its only predictors in the model.

We then examined the standardized path coefficients for each group. A bootstrapping procedure with 10,000 samples [26] was used to calculate the path significance. Statistical significance criteria for the path coefficients is determined by the bootstrapped standardized t statistic [7]: >3.291, significant at 0.1% (alpha = 0.001) probability of error; >2.576, significant at 1% (alpha = 0.01), >1.96, significant at 5% (alpha = 0.05) (two-tailed). The results of the analysis are shown in Table 2 for the privacy-enhancing app group and Table 3 for the non-privacy-enhancing app group.

The results for the privacy-enhancing app group show that only two relationships were not statistically significant: Trust did not have an effect on Intention to use and Disposition to value privacy did not have an effect on Perceived benefit of the app. In addition, Disposition to value privacy increased both Perceived risk and Intention to use the privacy-enhancing app, and it reduced Trust in the app. The same was true for Prior privacy experience, which in addition also significantly increased Perceived benefit of the privacy-enhancing app. On the other hand, for the non-privacy-enhancing app group the results show that Perceived risk did not have a significant effect on Intention to use the app. In addition, the covariates had a reduced influence. Disposition to value privacy and Prior privacy experience only significantly influenced Perceived risk and Trust. The result models are shown in Figure 3. With regards to indirect effects, Perceived risk and benefit both significantly mediated the effect of Trust on Intention to use the privacy-enhancing app. In addition, Trust mediated a negative effect of Disposition to value privacy on Perceived benefit. For the non-privacy-enhancing

Table 2. Path coefficients - Privacy-enhancing app group.

	Original Sample	Sample Mean	Std.Dev.	95% CI	T Statist.	p-value
Risk → Intention	−0.282	−0.279	0.114	[−0.497, −0.047]	2.460	**0.014**
Benefit → Intention	0.397	0.394	0.098	[0.194, 0.579]	4.042	**0.000**
Benefit → Risk	−0.174	−0.174	0.058	[−0.293, −0.062]	2.985	**0.003**
Trust → Intention	0.176	0.181	0.119	[−0.047, 0.421]	1.472	0.141
Trust → Benefit	0.704	0.704	0.047	[0.600, 0.787]	14.967	**0.000**
Trust → Risk	−0.494	−0.495	0.075	[−0.635, −0.341]	6.594	**0.000**
DispPriv → Intention	0.179	0.179	0.063	[0.055, 0.304]	2.817	**0.005**
DispPriv → Benefit	−0.077	−0.078	0.061	[−0.195, 0.040]	1.273	0.203
DispPriv → Risk	0.238	0.237	0.049	[0.145, 0.339]	4.880	**0.000**
DispPriv → Trust	−0.160	−0.158	0.078	[−0.311, −0.006]	2.041	**0.041**
ExpPriv → Intention	0.124	0.127	0.062	[0.005, 0.250]	1.998	**0.046**
ExpPriv → Benefit	0.153	0.153	0.067	[0.025, 0.289]	2.294	**0.022**
ExpPriv → Risk	0.222	0.222	0.061	[0.105, 0.343]	3.658	**0.000**
ExpPriv → Trust	−0.207	−0.212	0.092	[−0.380, −0.020]	2.250	**0.025**

Table 3. Path coefficients - Non-privacy-enhancing app group.

	Original Sample	Sample Mean	Std.Dev.	95% CI	T Statist.	p-value
Risk → Intention	0.021	0.021	0.127	[−0.239, 0.254]	0.170	**0.865**
Benefit → Intention	0.360	0.362	0.089	[0.184, 0.530]	4.054	0.000
Benefit → Risk	−0.144	−0.144	0.062	[−0.265, −0.019]	2.317	**0.021**
Trust → Intention	0.365	0.364	0.119	[0.122, 0.590]	3.078	**0.002**
Trust → Benefit	0.665	0.663	0.054	[0.549, 0.763]	12.242	**0.000**
Trust → Risk	−0.512	−0.511	0.066	[−0.635, −0.374]	7.719	**0.000**
DispPriv → Intention	−0.026	−0.025	0.083	[−0.183, 0.142]	0.310	0.757
DispPriv → Benefit	−0.123	−0.125	0.075	[−0.268, 0.022]	1.645	0.100
DispPriv → Risk	0.316	0.317	0.060	[0.204, 0.438]	5.294	**0.000**
DispPriv → Trust	−0.274	−0.272	0.082	[−0.425, −0.105]	3.333	**0.001**
ExpPriv → Intention	0.049	0.048	0.067	[−0.081, 0.181]	0.724	0.469
ExpPriv → Benefit	0.098	0.097	0.071	[−0.039, 0.235]	1.390	0.164
ExpPriv → Risk	0.103	0.103	0.052	[0.002, 0.207]	1.983	**0.047**
ExpPriv → Trust	−0.203	−0.208	0.080	[−0.348, −0.032]	2.554	**0.011**

app, Trust mediated the effect of the covariates on Perceived benefit and Intention to use.

Finally, we conducted the multigroup analysis procedure (PLS-MGA), which can test moderation by the group variable across the model, to evaluate the differences in the strength of the variables' relationships between experiment groups. The results show that the relationship between Disposition to value privacy and Intention to use (difference in path coefficient = -0.303, p=0.08), and Perceived risk and Intention of use (difference in path coefficient = 0.204, p=0.051) had the largest differences in path coefficient strength with $p < 0.1$. However, the differences were not significant at $p < 0.05$. This may be result of

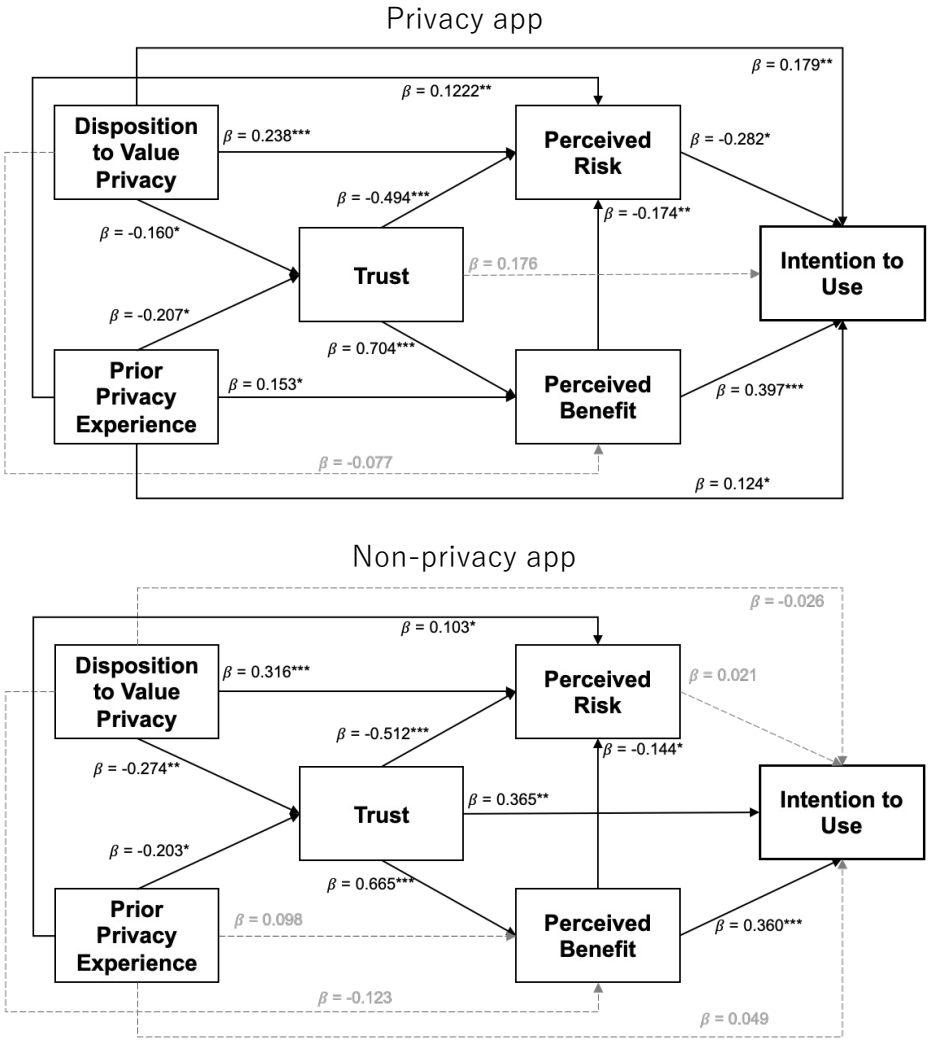

Fig. 3. Result models. Top: Privacy-enhancing app group. Bottom: Non-privacy-enhancing app group.

insufficient power for PLS-MGA: although the sample size per group is adequate for the separate analyses, the sample size is lower than the recommended sample size per group of 200 for multigroup analysis [17].

4 Discussion

As already known from previous research, one of the main factors of the intention to use an app are the perceived benefits (named performance expectancy in

UTAUT2) [31]. Thus, it is not surprising to identify that also in our experiment. If the tool is not perceived as beneficial, one wouldn't expect the (potential) users to use it. However, for those users who have an interest in using such a tool, there will be other factors contributing to and obstacles reducing the intention to use.

In our model, those factors are the perceived risk of the app and the trust in the app. Although participants perceive the same level of privacy-related risk towards both apps, an increase of perceived risk is not associated with a decrease of intention to use the non-privacy-enhancing app. In contrast, for the privacy-enhancing app, higher perceived privacy risk does have a significant negative influence on intention to use. In other words, the findings suggest that for the non-privacy-enhancing app, participants opinions follow along the privacy paradox, which states that privacy issues are considered important to users but that it does not affect their subsequent choices. Instead, other considerations, such as benefit, are more important to their actual behavior [19]. The results show that this does not happen for the privacy-enhancing tool. Considering that the hypothetical apps work in the same way and are almost identical except for their stated purpose, we can say this is a result of the experiment priming since the participants' are aware of the privacy-related purpose of the app. Regarding trust in the app, interestingly there is no significant direct influence from trust to intention to use for the privacy-enhancing app. While previous findings showed a direct effect [9–11], it seems that in our experiment the effect of trust on intention to use for the privacy-enhancing app was to a large degree mediated by perceived risk and perceived benefits. Similarly to perceived risks, disposition to value privacy increases both intention to use and perceived risk towards the privacy-enhancing app. This is a logical relationship, but the findings suggest a challenge for the adoption of this type of privacy-enhancing apps, which rely on user data processing, by people who are concerned about their privacy.

The result of our experiment shows that privacy-enhancing tools seem to prime users simply by stating their purpose, even though they would not fundamentally work differently than apps for other purposes. Naturally, it is difficult for privacy-enhancing tools to avoid priming users since tools need to have a proper name, often including privacy-related terms, to be found and of course described properly to let the (potential) users know what the tools are good for. If privacy terms were avoided, then those who are more disposed to think of privacy as important could fail to find these tools. On the other hand, as the findings show, the disposition to think that privacy as important has contrary effects: these users might want to use such tools to protect their privacy but at the same time feel increased privacy risk regarding the tool. Summing up, providers offering a privacy enhancing-tool should emphasize the privacy aspects. However, they should not only focus on explaining the benefits of their tool, but also trying to explain how their tool addresses potential risks of abusing user data to build trust. We encourage further research on how emphasizing these benefits and the risk mitigation, which are likely to be privacy-related, have additional impact on users' privacy risk perception.

4.1 Limitations

This study has a number of limitations. First, we are considering a parsimonious research model, and it is possible that other constructs may also affect intention to use, and that those relationships could be affected by the type of app. Second, we relied on the responses from Amazon Mechanical Turk workers. Research has shown that these workers have a higher sensitivity to privacy issues [16], and we also limited participation to experienced workers with a minimum of 5k tasks. Therefore, the results might not be generalizable to other populations. Third, we used a non-interactive app mockup for the experiment. This decreases the realism of the situation for participants, who are not risking their private information. Future research should consider validating these results in a more realistic situation, i. e. by investigating user perception of a real privacy-enhancing app.

5 Conclusions

In this study, we investigated whether user perception of a privacy-enhancing photo app is different from perception of a similar app that does not have a privacy purpose. The results show that there are differences in the relationships between privacy-related factors and intention to use the two types of app. Specifically, perceived risk does not have a significant influence on intention to use the non-privacy-enhancing app, which is congruent with the privacy paradox. However, for the privacy-enhancing app, perceived risk significantly negatively influences intention. In addition, although participants' disposition to value privacy positively influences how much risk they perceive towards the two types of apps, for the privacy-enhancing app it also has a positive influence on intention. That is, that the same disposition has a contrary effect of participants wanting to use the privacy-enhancing app, which would protect their privacy, and increasing how much privacy risk they feel from potentially using the app. In future research, we plan to experimentally investigate if the manipulation of the levels of these constructs might alter the balance between them in a way that results in increased or decreased intention to use a privacy-enhancing tool.

References

1. Bracamonte, V., Pape, S., Loebner, S.: "All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. Proc. Priv. Enhancing Technol. **2022**(3) (2022)
2. Bracamonte, V., Tesfay, W.B., Kiyomoto, S.: Towards Exploring User Perception of a Privacy Sensitive Information Detection Tool. In: 7th International Conference on Information Systems Security and Privacy (2021)
3. Corner, M., Dogan, H., Mylonas, A., Djabri, F.: A Usability Evaluation of Privacy Add-ons for Web Browsers. In: Marcus, A., Wang, W. (eds.) Design, User Experience, and Usability. Practice and Case Studies. pp. 442–458. Lecture Notes in Computer Science, Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-23535-2_33

4. Dijkstra, T.K., Henseler, J.: Consistent Partial Least Squares Path Modeling. MIS Quarterly **39**(2), 297–316 (2015)
5. Dinev, T., McConnell, A.R., Smith, H.J.: Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. Information Systems Research **26**(4), 639–655 (Dec 2015). https://doi.org/10.1287/isre.2015.0600
6. Dinev, T., Xu, H., Smith, J.H., Hart, P.: Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems **22**(3), 295–316 (May 2013). https://doi.org/10.1057/ejis.2012.23
7. Hair, J., Hult, G.T.M., Ringle, C., Sarstedt, M., Danks, N., Ray, S.: Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook (Nov 2021)
8. Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M.: When to use and how to report the results of PLS-SEM. European business review (2019)
9. Harborth, D., Pape, S.: How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies – the case of tor. In: 52nd Hawaii International Conference on System Sciences (HICSS) 2019. pp. 4851–4860 (01 2019). https://doi.org/10125/59923, https://scholarspace.manoa.hawaii.edu/handle/10125/59923
10. Harborth, D., Pape, S.: How privacy concerns, trust and risk beliefs and privacy literacy influence users' intentions to use privacy-enhancing technologies - the case of tor. ACM SIGMIS Database: the DATABASE for Advances in Information Systems **51**(1), 51–69 (01 2020). https://doi.org/10.1145/3380799.3380805, https://dl.acm.org/doi/abs/10.1145/3380799.3380805
11. Harborth, D., Pape, S., Rannenberg, K.: Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and jondonym. Proceedings on Privacy Enhancing Technologies (PoPETs) **2020**(2), 111–128 (05 2020). https://doi.org/10.2478/popets-2020-0020, https://content.sciendo.com/view/journals/popets/2020/2/article-p111.xml
12. Hasan, R., Crandall, D., Fritz, M., Kapadia, A.: Automatically Detecting Bystanders in Photos to Reduce Privacy Risks. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 318–335 (May 2020). https://doi.org/10.1109/SP40000.2020.00097
13. Henseler, J.: PLS-MGA: A non-parametric approach to partial least squares-based multi-group analysis. In: Challenges at the Interface of Data Analysis, Computer Science, and Optimization, pp. 495–501. Springer (2012)
14. Henseler, J., Ringle, C.M., Sarstedt, M.: Testing measurement invariance of composites using partial least squares. International marketing review (2016)
15. Jarvenpaa, S.L., Tractinsky, N., Saarinen, L.: Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer-Mediated Communication **5**(2), JCMC526 (Dec 1999). https://doi.org/10.1111/j.1083-6101.1999.tb00337.x
16. Kang, R., Brown, S., Dabbish, L., Kiesler, S.: Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In: 10th Symposium On Usable Privacy and Security ({SOUPS} 2014). pp. 37–49 (2014)
17. Klesel, M., Schuberth, F., Henseler, J., Niehaves, B.: A test for multigroup comparison using partial least squares path modeling. Internet Research **29**(3), 464–477 (Jan 2019). https://doi.org/10.1108/IntR-11-2017-0418
18. Kock, N., Hadaya, P.: Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. Information systems journal **28**(1), 227–261 (2018)

19. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security **64**, 122–134 (2017)
20. Korayem, M., Templeman, R., Chen, D., Crandall, D., Kapadia, A.: Enhancing Lifelogging Privacy by Detecting Screens. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 4309–4314. CHI '16, Association for Computing Machinery (May 2016). https://doi.org/10.1145/2858036.2858417
21. Li, Y., Vishwamitra, N., Knijnenburg, B.P., Hu, H., Caine, K.: Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. Proceedings of the ACM on Human-Computer Interaction **1**(CSCW), 67:1–67:24 (Dec 2017). https://doi.org/10.1145/3134702
22. Lin, T.Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., Zitnick, C.L.: Microsoft COCO: Common Objects in Context. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) Computer Vision – ECCV 2014. pp. 740–755. Lecture Notes in Computer Science, Springer International Publishing (2014). https://doi.org/10.1007/978-3-319-10602-1_48
23. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research **15**(4), 336–355 (Dec 2004). https://doi.org/10.1287/isre.1040.0032
24. Pavlou, P.A.: Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International journal of electronic commerce **7**(3), 101–134 (2003)
25. Ringle, C.M., Wende, S., Becker, J.M.: SmartPLS 3 (2015)
26. Sarstedt, M., Hair, J.F., Ringle, C.M., Thiele, K.O., Gudergan, S.P.: Estimation issues with PLS and CBSEM: Where the bias lies! Journal of Business Research **69**(10), 3998–4010 (2016)
27. Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., Cranor, L.F.: Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern. In: Proceedings 2016 Workshop on Usable Security. Internet Society (2016). https://doi.org/10.14722/usec.2016.23017
28. Sleeper, M., Cranshaw, J., Kelley, P.G., Ur, B., Acquisti, A., Cranor, L.F., Sadeh, N.: "i read my Twitter the next morning and was astonished": A conversational perspective on Twitter regrets. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 3277–3286. CHI '13, Association for Computing Machinery (Apr 2013). https://doi.org/10.1145/2470654.2466448
29. Smith, H.J., Milberg, S.J., Burke, S.J.: Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly **20**(2), 167–196 (1996). https://doi.org/10.2307/249477
30. Spiel, K., Haimson, O.L., Lottridge, D.: How to do better with gender on surveys: A guide for HCI researchers. Interactions **26**(4), 62–65 (Jun 2019). https://doi.org/10.1145/3338283
31. Venkatesh, V., Thong, J.Y., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly pp. 157–178 (2012)
32. Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G., Cranor, L.F.: "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. pp. 1–16. SOUPS '11, Association for Computing Machinery (Jul 2011). https://doi.org/10.1145/2078827.2078841
33. Xu, H., Dinev, T., Smith, J., Hart, P.: Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems **12**(12) (Dec 2011). https://doi.org/10.17705/1jais.00281