Comparing the Effect of Privacy and Non-Privacy Social Media Photo Tools on Factors of Privacy Concern

Vanessa Bracamonte[1], Sebastian Pape[2] and Sascha Loebner[2]
[1]*KDDI Research, Inc., Saitama, Japan*
[2]*Goethe University Frankfurt, Frankfurt am Main, Germany*

Keywords: Privacy Tools, Perceived Value of Information, Affect, Social Presence, Trust, Privacy Concern, User Study.

Abstract: Research into privacy tools for social media content has found that although there is a positive attitude towards these tools, there are also privacy concerns related to the user information involved. This privacy concern towards privacy tools can be higher than for non-privacy tools of a similar type, but the reason for this difference is not clear. To address this, we conducted an online experiment to compare the effect of a privacy and a non-privacy tool on antecedent factors of privacy concern (Perceived value of personal information, Social presence, Affect and Trust) which are hypothesized to be affected by the different purpose of the tools. The results show that participants had higher affect towards the privacy tool compared to the non-privacy tool. On the other hand, the results also show that participants in the privacy tool group had a higher level of perception of value of their personal information, that is, that the information provided to and inferred by the tool is valuable. Finally, both factors mediated a significant but opposing effect of the type of tool on privacy concern.

1 INTRODUCTION

Automated analysis of images has been proposed as a way of protecting peoples' privacy in a social media context (Korayem et al., 2016). In general terms, these proposals work by analyzing the content of users' photos to detect whether the content reveals private or sensitive information and potentially transforming that content to anonymize it (Ilia et al., 2015; Li et al., 2019; Hasan et al., 2020). Research has identified that users worry about their data being collected, sold, shared or misused, and about having their privacy intruded upon by these privacy tools (Bracamonte et al., 2021; Bracamonte et al., 2022). Although in essence this type of privacy tool would not be very different from a tool that analyzes users' content for the purposes of enjoyment, research has found that privacy concerns towards privacy tools can be higher than towards tools that would also analyze user data, but which have a non-privacy related purpose (Bracamonte et al., 2022). This indicates that the priming of the privacy tool has an effect on privacy concerns, but it is unclear through which mechanisms these effects are occurring.

We hypothesize that a number of factors may have a different effect on privacy concern towards privacy tools compared to non-privacy tools, and conduct an online survey-based experiment comparing the perception of two tools with similar characteristics but a different purpose: a tool for privacy vs. a non-privacy tool for enjoyment. In this paper, we evaluate possible constructs through which the positive and negative perceptions may be influencing privacy concern: Perceived value of personal information, Affect and Trust towards the tool, and Social presence.

2 RELATED WORK

Research on perception towards privacy tools that process personal data has identified that users have privacy concerns towards these types of tools. (Bracamonte et al., 2022) conducted a study comparing privacy and non-privacy tools for text and photos, and found that these concerns can be higher than for similar tools with a non-privacy related purpose. They also found that similar themes are reported when explaining the reasons for privacy concern towards both types of tools.

However, existing research has not evaluated through which mechanism do privacy tools influence privacy concerns differently than non-privacy tools. Nevertheless, findings from user evaluation studies of

Bracamonte, V., Pape, S. and Loebner, S.
Comparing the Effect of Privacy and Non-Privacy Social Media Photo Tools on Factors of Privacy Concern.
DOI: 10.5220/0011784900003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 669-676
ISBN: 978-989-758-624-8; ISSN: 2184-4356

privacy tools suggest some possibilities of variables which may explain this difference.

2.1 Perceived Value of Information

Privacy tools can cause some users to become concerned about how the tool itself may obtain value from the data they collect. (Schaub et al., 2016) found that users have reported concerns that privacy tools could potentially profit from their personal information (Bracamonte et al., 2022) similarly found that some users were concerned that a privacy tool could profit from their information through advertising, sharing or selling of the data.

When users become aware that their personal information is valuable to third parties, this can cause them to place a higher value on that information (Spiekermann et al., 2012). (Danezis et al., 2005) found that students increased their bids for the disclosure of their location information after learning that there was a possible commercial interest in that data. (Staiano et al., 2014) found that aggregated personal identifiable information, collected over a period of time, was valued higher than individual points of data , and it was hypothesized that the higher valuation was due to the participants realizing that this data revealed more information about their life.

A privacy tool such as the one described in this paper would work by detecting whether the information contained in the users' photos may be privacy sensitive. Therefore, the tool itself assigns some meaning to the content of the photo, which the users' may not have been aware of in advance. In doing so, the tool may be indicating that the information in the photo is something valuable to be protected. (Bracamonte et al., 2022) found that users appear to be concerned not only about the data collection aspect, but also what the privacy tool could gain from the data. If the photos are something to be protected, rather than "normal" photos, then it is possible that users would consider that data more valuable, to themselves or to others who would profit from it. This could result in an increased perception of the value of personal information, in comparison with tools that do not have a privacy-enhancing purpose. The privacy tool's inference or prediction of the users' content as (potentially) privacy sensitive may increase the perception of how valuable the content is, since the tools indicates it needs to be protected.

2.2 Social Presence

Social presence has been investigated as an influence on the positive perception of technology. (Gefen and Straub, 2004) indicate that social presence can have effect of perception in situations of interaction with technology where there is typically no direct interaction with a person. For example, the sense that others are present helps increase factors such as perceived trust (Gefen and Straub, 2004; Kim et al., 2013; Hassanein and Head, 2005) and benefit (Kim et al., 2013). The effect of social presence is present in different types of contexts of technology mediation, from websites (Gefen and Straub, 2004) to automation technology such as robots (Kim et al., 2013), to varying degrees. Much of the research has focused on the effect of human images, but research by (Hassanein and Head, 2005) has shown that interfaces that evoke emotions such as fun or interest can also increase the perception of social presence.

An utilitarian tool such a tool for privacy may not have as much social presence, in the sense of positive human connection, in comparison with a tool for enjoyment. In addition, (Oh et al., 2018) report that social presence is not always correlated with positive effects, and that its effects may depend on the context, such as when a person is vulnerable. It is likely that users would imagine different contexts for the use of privacy vs. non-privacy tools. In a privacy context, users may feel vulnerable and social presence could represent a risk rather than a benefit.

2.3 Affect and Trust

It is also important to consider that not only negative perceptions could affect privacy concern. A privacy tool such as the one in the current study only differs from a non-privacy tool in its purpose, and because the purpose is privacy protection or enhancement, which benefits the user, this may result in positive perception. (Dinev et al., 2015) indicate that privacy concerns are not only influenced by analytical processes, but are also affected by dispositional attitudes. Extraneous influences have an effect on privacy concerns, and positive or negative feelings and heuristics are also used used in order to decide and make privacy judgments about a particular technology. Users have positive feelings towards privacy tools due to their purpose of protection (Schaub et al., 2016; Bracamonte et al., 2021). Positive feelings, influenced by the beneficial purpose of this type of tools, could also work to reduce concerns. (Schaub et al., 2016) indicated that users had a feeling of protection by the privacy tool, and that this mitigated concerns related

to tracking. (Bracamonte et al., 2022) found that the purpose of the privacy tool was mentioned as one of the reasons for having a lower level of privacy concern, whereas there was no such reason for the non-privacy tool. The privacy tool, which purpose is to protect users, could increase positive feelings in users.

Positive feelings, or Affect, can be defined as thought of as automatic responses associated with a stimulus (Slovic et al., 2002). If we compare a privacy and non-privacy tool, we can take the privacy purpose of the former as a stimulus that primes users for a type of reaction or response. Therefore, in their initial interaction with a privacy tool, positive perception of the privacy tool brought by feelings of protection may increase affect towards it, compared to a non-privacy tool. Furthermore, (Finucane et al., 2000) and (Slovic et al., 2002) indicate that overall affective evaluation of an object can influence the risk judgment related to that object. For example, (Kehr et al., 2015) found that positive feelings towards a technology medium can influence people's privacy assessment and can result in underestimating information disclosure risks. Another factor which can automatically affected by stimulus is trust (Lindgaard et al., 2006). (Gefen and Straub, 2004) indicate that trust plays an important role in the perception of technology, and it is considered important for privacy tools as well (Balebako et al., 2013; Coopamootoo, 2020; Harborth et al., 2020).

3 METHODOLOGY

3.1 Research Questions

The objective of the paper is to evaluate the mechanism through which a privacy tool affects privacy concern differently from a non-privacy tool, focusing specifically on tools for the analysis and transformation of social media photos. We propose a number of factors to test, and evaluate the following research questions:

R1: Are the levels of Perceived value of information, Social presence, Affect and Trust different when viewing a privacy tool compared to viewing a non-privacy tool?

R2: Does the privacy tool have a different effect (compared to the non-privacy tool) on Privacy concern through those variables? That is, do Perceived value of information, Social presence, Affect and Trust mediate the effect of the type of tool on Privacy concern?

3.2 Experiment Design

In order to answer the research questions, we designed an experiment which consisted of a task for participants to view, read a description and give their opinion about an hypothetical app that would be used to transform photos for uploading on social media. We manipulated the type of tool that the participants viewed: a privacy tool or a non-privacy tool for social media photos. The objective of this study was to evaluate differences in perception that resulted from the manipulation (priming), therefore, the privacy tool 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.

3.3 Task

We described to participants an hypothetical free, third-party app for social media photos. For the privacy tool, the purpose was described as protecting privacy; for the non-privacy tool, 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 privacy tool, and information that could be enhanced with stickers for the non-privacy tool. We then presented a non-interactive mockup of the app interface which showed how it would work. The mockups for each group had the same general design, and only differed in their message ("Privacy alert!" vs "Enhance it!") and the transformation performed on the photo (privacy-enhancing vs non-privacy-enhancing).

After the mockup, we showed five additional photo examples to the participants. The photos for the examples were obtained from the COCO dataset (Lin et al., 2014).

3.4 Measurement Items

We included items adapted from previous research to measure Social presence (Gefen and Straub, 2004) and Affect (Kehr et al., 2015). The items for measuring Perceived value of information were developed based on the single-item measurement from (Spiekermann et al., 2012), adapted to refer to personal information provided by the user and personal information generated by the tool. Privacy concern was measured with the Mobile Users' Information Privacy Concerns (MUIPC) scale, which is comprised of the dimensions of Perceived surveillance, Perceived intrusion

and Secondary use of personal information (Xu et al., 2012). Trust was measured with 3 items adapted from (Jarvenpaa et al., 1999). All questions had a 7-point response scale, from *Strongly disagree* to *Strongly agree*, with the exception of the Affect items.

To validate that the samples in each group were comparable, we included questions on Prior privacy experience (Smith et al., 1996), Disposition to value privacy (Xu et al., 2011), Information sensitivity (Dinev et al., 2013), as well as questions on the participants' age, gender (as an open text box (Spiel et al., 2019)) and frequency of social media posting, in general and for photos in particular. The questionnaire also included open-ended attention check questions, where we asked participants to answer briefly about the app described.

3.5 Ethical Considerations

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 that 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 researcher's 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.

3.6 Participant Recruitment

We recruited participants by posting a task to answer a survey on Amazon Mechanical Turk. We set the qualifications for participation for workers from the USA, who had a 99% rate of acceptance rate for their tasks and who had worked on at least 5000 tasks. We set the participant reward at US$2.5.

The survey ran on February 8-9, 2022. We obtained 400 responses in total. We reviewed the answers to all open-ended questions to identify cases with multiple nonsensical answers or answers which were completely unrelated to the questions. We identified 20 such responses, and rejected them. The rest of the participants were rewarded, at a rate of US$12.5/hour. The median response time was 12 minutes.

4 RESULTS

In this section, we describe the analysis method (PLS-SEM) we used, then report the final sample characteristics, the measurement model's reliability and validity analysis results, and finally the results of the structural model analysis.

To evaluate the research questions of this study, we used the partial least squares structural equation modeling (PLS-SEM) method. In summary, the PLS-SEM method consists of a series of steps from checking the reliability of the measurement model (relationship between the measurement items and its corresponding construct), the reliability of the structural model (relationships between the constructs) and finally obtaining the path coefficients (direct and mediated) i.e. the relationships between the constructs (Hair et al., 2019).

We conducted the PLS-SEM analyses using the R seminr package (Ray et al., 2022).

4.1 Sample Characteristics

The sample consisted of 380 cases. We first identified 22 multivariate outliers, using the Mahalanobis distance (alpha = 0.001), and removed them. We reviewed the answers to the attention questions, but found none that could be considered incorrect. The final sample for analysis consisted of 358 participant responses, 179 in each group. The sample size obtained was over the minimum for finding path coefficients of 0.11 - 0.2 with a 1% significance level and a power of 80% with the PLS-SEM method (Hair et al., 2021), according to guidelines based on the inverse square root method for minimum sample size estimation (Kock and Hadaya, 2018). The age mean was 41 years-old for both groups. The gender distribution was 53% female / 48% male participants in the privacy tool group, and 56% female and 44% male in the non-privacy tool group.

Mann-Whitney U tests indicated no significant differences in age (W = 16124, p-value = 0.92) frequency of social media posting, in general (W = 17594, p-value = 0.10) or photos in particular (W = 17446, p-value = 0.14), Prior privacy experience (W

= 14904, p-value = 0.25), Disposition to value privacy (W = 14960, p-value = 0.28) or Information sensitivity (W = 15230, p-value = 0.42) between groups.

4.2 Measurement Model

We first evaluated the reliability and validity of the measurement model. The PLS-SEM method can be used to evaluate multiple relationships simultaneously, so in addition to the relationships related to the research questions, we also control for the effects of constructs which have been validated in previous research, such as the influence on Social presence on Trust (Gefen and Straub, 2003), but we do not focus on those in this paper.

An initial evaluation indicated that although all other reliability indicators were satisfactory, the constructs of Perceived surveillance, Intrusion and Secondary use of personal information had low discriminant validity. These constructs are dimensions of Privacy concern (Xu et al., 2012), and therefore conceptually similar. Therefore, we modeled Privacy concern as a higher-order construct and report the results of the evaluation of the higher-order measurement model. We examined indicator reliability by inspecting the values obtained by squaring the item loadings, which are the correlation weights between the construct and its indicators (measurement items). All items had an indicator value (squared loading) over the threshold of .708 (Hair et al., 2019).

To evaluate internal consistency reliability, which is the association between indicators of the same construct, we examined the Cronbach's alpha and the rhoA reliability coefficient (Dijkstra and Henseler, 2015). For all constructs, Cronbach's alpha values ranged from 0.932 - 0.973, and rhoA values ranged from 0.932 - 0.973, which is higher than the satisfactory minimum of 0.7 (Hair et al., 2021). Although reliability coefficient values were higher than the ideal upper limit of 0.9, this is likely due to the use of established scales.

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 (Hair et al., 2019), on a range from 0.856 - 0.949. Finally, we examined the discriminant validity, which is how much a construct is distinct from other constructs, using the heterotrait–monotrait (HTMT) ratio of correlations criterion. All values were significantly lower than the threshold value of 0.9 (Hair et al., 2021).

4.3 Structural Model

After validating the measurement model, we assessed the structural model. We first examined whether there were collinearity issues (too high correlation between constructs) in the structural model, by calculating the variance inflation factor (VIF) values for the constructs. All VIF values were below the minimum recommended of 3 (Hair et al., 2021), with values ranging from 1.01 - 2.11. We then examined the R-squared values, which measure the variance in a construct explained by the predictors; values of 0.25 are considered weak (Hair et al., 2019). Social presence and Perceived value of information were the only constructs with a value lower than 0.25, but this is expected since the type of tool is their only predictor in the model. All other values were above the moderate threshold of 0.5 (Hair et al., 2019).

The structural model included the experiment groups as a dichotomous variable (1 for the privacy tool and 0 for the non-privacy tool). We conducted a bootstrapping procedure with 10,000 samples (Sarstedt et al., 2016) to calculate the path significance. Statistical significance criteria in this case is determined by the bootstrapped standardized t statistic (Hair et al., 2021): above 3.291 corresponds to significant at 0.1% probability of error (alpha = 0.001) ; above 2.576, to significant at 1% (alpha = 0.01), and above 1.96, to significant at 5% (alpha = 0.05) (two-tailed). These are represented in the tables with * for significant at 5%, ** for 1%, and *** for 0.1%.

Figure 1 shows the representation of those results. The results, specifically the direct paths from the variable representing the tool, answer the first research question (R1) of whether the level of the factors is different for the privacy tool compared to the non-privacy tool group. The results show that Perceived value of information and Affect were significantly higher for the privacy tool. On the other hand, Social presence, Trust and also Privacy concern itself were not significantly different between the two groups. Although they are not the focus of this study, we observe from the results that other direct relationships between constructs were significantly different. However, one interesting result is that Social presence increases Privacy concern, but also increases Affect and Trust.

We then examined the mediated effects on Privacy concern (Table 1) to answer the second research question (R2). The results show that there was a significant indirect effect of the privacy tool on Privacy concern (compared to the non-privacy tool) through Perceived value of information, which resulted in an increase of Privacy concern. There was also a signif-

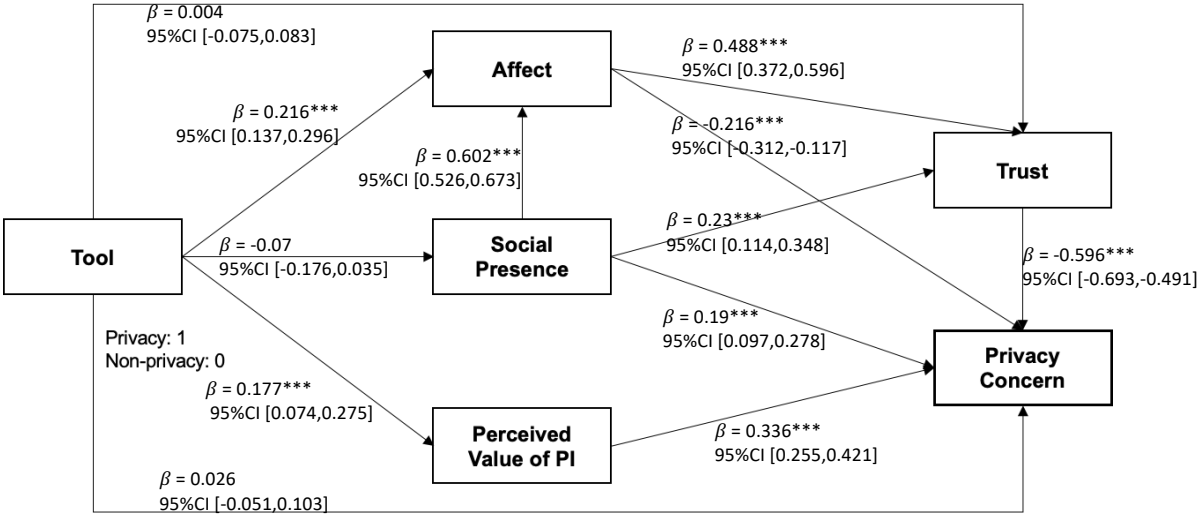

Figure 1: Results of the PLS-SEM analysis.

Table 1: Mediation effects results: standardized coefficients and significance.

X	Mediator(s)	Original Est	Bootstrap Mean	Bootstrap SD	T Stat.	95% CI	Signif.
Tool	Value	0.059	0.06	0.02	3.034	[0.023, 0.1]	**
Tool	SocialPresence	−0.013	−0.013	0.011	−1.193	[−0.037, 0.006]	
Tool	Affect	−0.047	−0.047	0.014	−3.376	[−0.077, −0.022]	***
Tool	Trust	−0.002	−0.003	0.024	−0.086	[−0.051, 0.043]	

icant mediated effect on Privacy concern through Affect which resulted in a decrease of Privacy concern. In line with the direct effect results, neither Trust nor Social presence significantly mediate the effect of the privacy tool on Privacy concern.

5 DISCUSSION

The results of the analysis indicate that privacy concern towards a privacy tool is affected through an increase of the perception of value of the information that the user gives the tool and the value of the information the tool infers from the photos, and through Affect and Trust towards the privacy tool, which is higher in comparison to the non-privacy tool. However, these variables have opposing effects on privacy concern. Affect decreased Privacy concern and acted as a mediator of the positive effect of Social presence on Privacy concern. In the opposite direction, an increased Perception of the value of personal information increased Privacy concern towards the tool, and countered the previously described effect. In this study, the result was that the overall effect the privacy tool on privacy concern (compared to the non-privacy tool) was not significant (unlike the findings by (Bracamonte et al., 2022)), as these two opposing effects canceled each other out.

We consider that the fact that users report a higher a level of Perceived value of information represents an interesting problem for privacy tools of the type we focus on in this study. We can assume that the provider of a such a tool would naturally want to emphasize the privacy protection aspect, and this may increase a positive attitude towards the tool. On the other hand, by emphasizing protection the providing may also be emphasizing the value of the data that is to be protected. Once that is established, users may be able to more easily imagine what would be the negative consequences of losing control of that data. Another possibility is that the provider could emphasize other aspects of the privacy tool besides the protection itself, in order to increase affect towards it.

Finally, although the results showed that the privacy tool did not significantly increase or decrease perception of Social presence compared to the non-privacy tools, Social presence directly increased Privacy concern and at the same time increased positive perceptions (Affect and Trust). This might indicate that a variable not included in this study may be mediating the effect of Social presence on Privacy Concern. Future research should validate empirically val-

idate these effects, since research has shown that the effect of Social presence can depend on the context of use of a technology (Phelan et al., 2016; Zhang and Xu, 2016; Mozafari et al., 2021).

5.1 Limitations

First, 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. Second, we only evaluated a limited set of variables that affect Privacy concern in this experiment. The results show that these variables explained Privacy Concern with an R-squared = 0.538 (moderate). Nevertheless, we acknowledge that there could be other variables which could also explain a difference in perception of these two types of tools. Third, we recruited Amazon Mechanical Turk workers for the experiment. Although research has found that these workers have a higher sensitivity to privacy issues (Kang et al., 2014), there is also evidence that privacy-related related knowledge matches the US population to some extent (Redmiles et al., 2019). Nevertheless, the results might not generalize to other populations.

6 CONCLUSIONS

Previous research has found evidence of a higher level of privacy concern towards privacy tools compared to similar tools with a non-privacy purpose. In this paper, we explore the mechanisms that might explain this difference in privacy concern. We found that privacy tools increased the Perception of value of personal information, and that this variable mediated an increase of Privacy concern caused by the privacy tool. We also found that the privacy tool increases Affect compared to the non-privacy tool, and that Affect along with Trust mediate a decrease of Privacy concern. In our study, these effects appeared to cancel each other out, resulting in an overall non-significant effect of the privacy tool on Privacy concern, compared to the non-privacy tool. Finally, we found no significant differences in the level of Trust and Social presence between the privacy and non-privacy tools, although these two variables had an effect on Privacy concern.

In future research, we plan to empirically examine how privacy tools affect the perception of value of information, and how this perception affects privacy concern in turn.

REFERENCES

Balebako, R., Jung, J., Lu, W., Cranor, L. F., and Nguyen, C. (2013). "Little Brothers Watching You": Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 1–11. Association for Computing Machinery.

Bracamonte, V., Pape, S., and Loebner, S. (2022). "All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. *Proc. Priv. Enhancing Technol.*, 2022(3).

Bracamonte, V., Tesfay, W. B., and Kiyomoto, S. (2021). Towards Exploring User Perception of a Privacy Sensitive Information Detection Tool. In *7th International Conference on Information Systems Security and Privacy*.

Coopamootoo, K. P. (2020). Usage Patterns of Privacy-Enhancing Technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, pages 1371–1390. Association for Computing Machinery.

Danezis, G., Lewis, S., and Anderson, R. (2005). How much is location privacy worth. In *In Proceedings of the Workshop on the Economics of Information Security Series (WEIS*.

Dijkstra, T. K. and Henseler, J. (2015). Consistent Partial Least Squares Path Modeling. *MIS Quarterly*, 39(2):297–316.

Dinev, T., McConnell, A. R., and Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, 26(4):639–655.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3):295–316.

Finucane, M. L., Alhakami, A., Slovic, P., and Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of behavioral decision making*, 13(1):1–17.

Gefen, D. and Straub, D. (2003). Managing user trust in B2C e-services. *e-Service*, 2(2):7–24.

Gefen, D. and Straub, D. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega*, 32:407–424.

Hair, J., Hult, G. T. M., Ringle, C., Sarstedt, M., Danks, N., and Ray, S. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European business review*.

Harborth, D., Pape, S., and Rannenberg, K. (2020). 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.

Hasan, R., Crandall, D., Fritz, M., and Kapadia, A. (2020). Automatically Detecting Bystanders in Photos to Reduce Privacy Risks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 318–335.

Hassanein, K. and Head, M. (2005). The impact of infusing social presence in the web interface: An investigation across product types. *International Journal of Electronic Commerce*, 10(2):31–55.

Ilia, P., Polakis, I., Athanasopoulos, E., Maggi, F., and Ioannidis, S. (2015). Face/off: Preventing privacy leakage from photos in social networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 781–792.

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication*, 5(2):JCMC526.

Kang, R., Brown, S., Dabbish, L., and Kiesler, S. (2014). Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 37–49.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus: Privacy calculus: Dispositions and affect. *Information Systems Journal*, 25(6):607–635.

Kim, K. J., Park, E., and Sundar, S. S. (2013). Caregiving role in human–robot interaction: A study of the mediating effects of perceived benefit and social presence. *Computers in Human Behavior*, 29(4):1799–1806.

Kock, N. and Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information systems journal*, 28(1):227–261.

Korayem, M., Templeman, R., Chen, D., Crandall, D., and Kapadia, A. (2016). Enhancing Lifelogging Privacy by Detecting Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4309–4314, New York, NY, USA. Association for Computing Machinery.

Li, F., Sun, Z., Li, A., Niu, B., Li, H., and Cao, G. (2019). HideMe: Privacy-Preserving Photo Sharing on Social Networks. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 154–162.

Lin, T.-Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., and Zitnick, C. L. (2014). Microsoft COCO: Common Objects in Context. In Fleet, D., Pajdla, T., Schiele, B., and Tuytelaars, T., editors, *Computer Vision – ECCV 2014*, Lecture Notes in Computer Science, pages 740–755. Springer International Publishing.

Lindgaard, G., Fernandes, G., Dudek, C., and Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! *Behaviour & information technology*, 25(2):115–126.

Mozafari, N., Weiger, W., and Hammerschmidt, M. (2021). *That's so Embarrassing! When Not to Design for Social Presence in Human-Chatbot Interactions*.

Oh, C. S., Bailenson, J. N., and Welch, G. F. (2018). A Systematic Review of Social Presence: Definition, Antecedents, and Implications. *Frontiers in Robotics and AI*, 5.

Phelan, C., Lampe, C., and Resnick, P. (2016). It's Creepy, But it Doesn't Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5240–5251. Association for Computing Machinery.

Ray, S., Danks, N. P., Valdez, A. C., Estrada, J. M. V., Uanhoro, J., Nakayama, J., Koyan, L., Burbach, L., Bejar, A. H. C., and Adler, S. (2022). Seminr: Building and Estimating Structural Equation Models.

Redmiles, E. M., Kross, S., and Mazurek, M. L. (2019). How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1326–1343.

Sarstedt, M., Hair, J. F., Ringle, C. M., Thiele, K. O., and Gudergan, S. P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research*, 69(10):3998–4010.

Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., and Cranor, L. F. (2016). Watching Them Watching Me: Browser Extensions Impact on User Privacy Awareness and Concern. In *Proceedings 2016 Workshop on Usable Security*. Internet Society.

Slovic, P., Finucane, M., Peters, E., and MacGregor, D. G. (2002). Rational actors or rational fools: Implications of the affect heuristic for behavioral economics. *The Journal of Socio-Economics*, 31(4):329–342.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167–196.

Spiekermann, S., Korunovska, J., and Bauer, C. (2012). Psychology of ownership and asset defense: Why people value their personal information beyond privacy. *Available at SSRN 2148886*.

Spiel, K., Haimson, O. L., and Lottridge, D. (2019). How to do better with gender on surveys: A guide for HCI researchers. *Interactions*, 26(4):62–65.

Staiano, J., Oliver, N., Lepri, B., de Oliveira, R., Caraviello, M., and Sebe, N. (2014). Money walks: A human-centric study on the economics of personal mobile data. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 583–594. ACM.

Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12).

Xu, H., Gupta, S., Rosson, M., and Carroll, J. (2012). Measuring Mobile Users' Concerns for Information Privacy. In *ICIS*.

Zhang, B. and Xu, H. (2016). Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, pages 1676–1690. Association for Computing Machinery.