Investigating Privacy Concerns Related to Mobile Augmented Reality Applications

Short Paper

David Harborth
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4,
60326 Frankfurt a.M., Germany
david.harborth@m-chair.de

Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4,
60326 Frankfurt a.M., Germany
sebastian.pape@m-chair.de

Abstract

Augmented reality (AR) gained much public attention since the success of Pokémon Go in 2016. Technology companies like Apple or Google are focusing primarily on mobile AR (MAR) applications running on smartphones or tablets since this type of AR is widely available for the end consumer. Associated privacy issues have to be investigated early as long as AR is still shapeable in order to improve users' privacy and foster market adoption. Thus, we designed a vignette-based online experiment to investigate influencing factors of privacy concerns related to a hypothetical MAR app. Furthermore, we investigate whether individuals associate higher privacy concerns with AR compared to non-AR by manipulating the description of the app. Thereby, we want to better understand the attitude formation process related to AR and the relation to privacy concerns. We conduct a pretest with 91 German smartphone users to evaluate the used constructs and our proposed research model.

Keywords: Mobile augmented reality, privacy concerns, app transparency, vignette-based experiment

Introduction

The release of Pokémon Go in 2016 led to a major boost in public awareness about augmented reality (AR) (Nicas and Zakrzewski 2016). An AR technology is defined as a system which "[…] combines real and virtual objects in a real environment; runs interactively, and in real time; and registers (aligns) real and virtual objects with each other" (Azuma et al. 2001, p. 34). Big technology companies recently engage heavily in acquisitions of AR companies (1.2 billion dollar in investment in the first half of 2017 (Simnett 2018)), showing the expectations associated with the technology to become a potential game changer. These expectations are well captured by a statement of Tim Cook implying that AR might become as ubiquitous and important as the smartphone today:

"*AR is going to take a while, because there are some really hard technology challenges there. But it will happen, it will happen in a big way, and we will wonder when it does, how we ever lived without it. Like we wonder how we lived without our phone today"* (Cook 2016).

This paper focuses on the end user in the B2C area. The two main types of AR are considered to be smart glasses and mobile AR (MAR) applications. AR glasses like the Microsoft Hololens (Microsoft 2017) are currently not mature enough, i.e. too intrusive to wear and too expensive for the end consumer market. This type of AR is primarily used in the B2B environment where it can be observed that AR saves time and costs (Kohn and Harborth 2018). Another way of presenting AR to the user is via smartphones or tablets (MAR). Pokémon Go is the most widely known example for this category. When Apple (ARKit) and Google (ARCore) released AR development kits in 2017, the AR features, like object tracking, started to become better (Nellis 2017) and many new MAR applications (apps) diffused into the consumer market.

Nowadays, the majority of people experience AR mainly by interacting with MAR apps on their mobile devices. This has the consequence that MAR apps can shape the perceptions of millions of users concerning AR in general.

We could see privacy issues arising with MAR apps (e.g. for Pokémon Go (Peterson 2016)) and research indicates that individuals are concerned about their privacy when using AR (Dacko 2017; Harborth 2019; Harborth and Pape 2018; Rauschnabel et al. 2018). Such privacy concerns and threats can be a hindering factor of technology adoption (Angst and Agarwal 2009; Slyke et al. 2006). Besides these findings related to user perceptions, there are technical assessments of risks related to AR which show that AR poses new privacy risks that should be addressed as early as possible (de Guzman et al. 2018; Harborth et al. 2019). Therefore, from a practical point of view, there is a clear need to investigate potential factors influencing the privacy concerns in order to address them as early as possible when developing respective MAR applications to enhance market adoption.

From a theoretical point of view, there is a lack of user studies in the IS domain investigating AR, and especially privacy in the context of AR (Harborth 2017). Addressing this research gap is especially important since context-specific privacy concerns can differ greatly from general privacy concerns (Ackerman and Mainwaring 2005). Therefore, we chose a vignette-based design in order to present participants a highly specified environment (in our case a mockup of an app store website for a hypothetical MAR app). Thus, besides adding to the research gap described before, we contribute to theory by analyzing whether privacy concerns affect download intentions and by developing a highly context-specific research model to investigate to what extent context-specific factors matter and relate to non-context-specific ones (e.g. privacy concerns related to the app vs. global information privacy concerns).

In summary, our research goal is to investigate differences in drivers of privacy concerns and download intentions of MAR apps compared to non-MAR apps. Thus, three research questions arise:

1. *What factors contribute to users' privacy concerns with respect to MAR apps?*
2. *Do users associate higher privacy concerns with a MAR app compared to a non-MAR app?*
3. *Do privacy concerns weaken the intention to download MAR applications?*

The remainder of the paper is structured as follows. We describe related work in Section 2. The methodology is described in Section 3 and the preliminary results are presented in Section 4. Section 5 concludes the short paper by outlining the next steps for this research project.

Related Work

There is a plethora of research on privacy threats and concerns related to the smartphone ecosystem. Research can be categorized by the user journey related to mobile apps. In the first stage, the user has to download the app. Secondly, the user installs the app. The last stage is the actual use of the app. Our research is located in the first stage, i.e. analyzing factors driving privacy concerns in the download stage, which ultimately influence the download intention. Research analyzing the download stage is relatively rare compared to the other stages (Gu et al. 2017). The comparable study Gu et al. 2017 finds that users' privacy concerns in the download stage are alleviated by the popularity of the app (the more people downloaded the app, the more trustworthy it is) and by the existence of permission justifications (explaining users why apps need certain permissions), although the latter effect becomes less relevant if users had prior negative privacy experiences. In addition, they find that users' privacy concerns increase if apps require more sensitive permissions. Overall, their model integrates relevant factors from the mobile ecosystem for explaining privacy concerns and the download intentions in the mobile app context, which is why we adapt their model to our case of MAR. Besides this study, Kelley et al. (2013) investigate the effect of presenting permissions clearly to the users in the download stage. They find that making permissions of an app clear and apparent helps users become aware of these permissions. Their results indicate that users would like to better understand why applications need certain information, whereas the authors did not include permission justifications in their study design.

There is a lot of research analyzing the installation stage. For example, prior findings suggest that users tend to disregard security alerts as most of them are not able to understand the risks and privacy issues associated with them (De Cristofaro 2011; Felt et al. 2012; Mylonas et al. 2013). In addition to this lack of understanding, users oftentimes do not care about privacy ("I've got nothing to hide"). In contrast to these findings, a study by Painter (2013) revealed that more than half of the users have decided to uninstall apps or abstain from installing it due to privacy concerns. Research investigating privacy issues during the actual runtime phase is concerned with privacy-invasive accesses of apps to smartphone resources (Hatamian et al. 2017). Prior research finds that MAR apps oftentimes misbehave with respect to privacy and do not follow the principle of least privilege. In addition, most resource accesses (e.g. to the phone's contacts or audio) are not covered by their respective privacy policies (Harborth et al. 2019).

Methodology

In this section, we discuss the vignette-based experiment design and develop the research hypotheses and the research model. In addition, we describe how we collected the initial sample for our pretest.

Experiment Design and Research Model Development

We address our research questions with a 2x2x2x2 between-subjects vignette-based online experiment. Participants were randomly assigned to one of the 16 different vignettes containing the respective combinations of information about a hypothetical MAR measurement app which allows users to measure distances between objects in the real environment. We chose this example since MAR measurement apps work very well and are widely diffused (e.g. Apple integrated such an app in iOS12 (Apple 2019)). In addition, participants can easily understand the use scenario of such an app (compared to a game which they do not know) and such apps are likely to be used in potentially privacy sensitive environments (e.g. at home or in the office). Participants were first introduced to a ranking page with the download numbers of the MAR app (first factor of the experiment). The app was either ranked on place three of 20 with 300,000 downloads or on place 18 with 800 downloads. After that, participants had to click on the name of our MAR app in order to be directed to the hypothetical app store with the overview page of the app. Here, we designed mockups containing the remaining 8 different manifestations for the requested permissions, justifications for why the permissions are needed and whether the app is clearly labelled as being "Augmented Reality" or not[1]. After seeing one mockup, participants continued by answering questions on their perceptions (cf. appendix). All questions related to the research model are randomized. We use this experiment design since certain treatments are binary variables in our model (permission justification, app labelled as AR) and in order to introduce variance in the variables about perceptions (permission sensitivity, app popularity and consequently privacy concerns).

The paper by Gu et al. (2017) serves as a theoretical starting point and we adapt the constructs *perceived permission sensitivity* (PS), *perceived app popularity* (PAP), *privacy concerns* (PC), *mobile privacy victim experience* (MPVE) and *download intentions* (DI) to our research context. As discussed in Section 2, their model fits very well to our research context and indicates significant relationships between the mentioned variables. However, we need to augment the original model by including the construct *attitudes towards AR* (adapted from Chen and Sharma (2015)) and controlling for AR-specific variables, i.e. whether participants know what AR is and exposing them to the AR labeled mockup or not. We include this construct related to attitudes since prior research indicates that individuals might associate negative perceptions and concerns with AR (Harborth 2019). In contrast, for certain technically affine users, AR is a new and exciting technology which could be perceived as positive. We include this general construct *attitudes towards AR* in the model in order to capture these potential effects.

Privacy concerns about the app in the download stage depend on PS, PJ, PAP and MPVE. The influence of these factors follows the notion that individuals form and change attitudes involving high or low levels of cognitive effort (elaboration likelihood model (ELM) (Petty et al. 1983)). *Permission sensitivity and justification* are assessed over the central route, i.e. involving a relatively high degree of elaboration and cognitive effort. Permissions basically represent information types. Prior research suggests that individuals deliberately think about information sensitivity which causes them to associate higher privacy

[1] see http://www.appresearchproject.pallas.net/appstore4e for an exemplary mockup containing all possible treatments (dangerous permissions, permission justification and AR label), and http://www.appresearchproject.pallas.net/appstore0e for the version without AR.

concerns with certain types of (more) sensitive information (Bansal et al. 2010). In contrast, *app popularity* is evaluated with a low degree of elaboration (peripheral route) since it represents a heuristic for individuals indicating that a product or service is trustworthy due to many prior adopters (Duan et al. 2009). However, the degree of elaboration can be influenced by motivation and ability (Bhattacherjee and Sanford 2006). Gu et al. (2017) suggest that past negative privacy experiences represent such a cause for individuals to be more motivated and, under certain circumstances, more able to deal with privacy-related information. In addition, individuals will be more concerned with respect to their privacy in general.

The concept of app popularity is similar to that of reviews with the difference that it only covers one dimension. The download numbers are a heuristic for the popularity and therefore indicate to people that many others before them downloaded this app. Thus, the app must be good or, at least, cannot be bad. In its current form, app popularity should influence privacy concerns as follows:

H1: Perceived app popularity negatively influences the privacy concerns related to the intention to download the MAR app.

We designed the permission justifications in a way that they explain even the dangerous and unnecessary permission requests of the MAR app. For example, one could argue that a measurement app does not need access to the microphone. Here, we developed a justification stating that users can add audio notes to each measurement file and, therefore, easily annotate it. Thus, we expect that such explanations alleviate the privacy concerns:

> *H2: The existence of permission justifications negatively influences the privacy concerns related to the intention to download the MAR app.*

Permission sensitivity has two manifestations. Either the participants see only three regular permissions requested by the app (camera, storage, others) or they see six permissions including the three prior ones and three additional dangerous permissions (location, contacts, microphone). We chose these permissions according to the Android developer guide about different permission types (Android Developers 2019). Camera is also classified as a dangerous permission. However, since our hypothetical app is an MAR app either way, we included the camera permission in every manifestation. The idea of including this concept stems from past research indicating that privacy concerns are influenced by information sensitivity (Bansal et al. 2010). Thus, it can be hypothesized that:

> *H3: Perceived permission sensitivity positively influences the privacy concerns related to the intention to download the MAR app.*

As described before, past negative privacy experiences (MPVE) influence the extent of elaboration since individuals might be more motivated and able to deal with privacy-related information if they had to deal with privacy breaches in their past. In addition, such experiences lead to higher privacy concerns among the affected individuals (Smith et al. 2011). If such individuals are more concerned and scrutinize over their privacy-related decisions, all variables which positively influence privacy concerns are amplified and all variables which alleviate privacy concerns are weakened. Thus, we hypothesize the following:

> *H4: MPVE will moderate the effect of the perceived permission sensitivity on the privacy concerns, such that the effect will be stronger for individuals with high levels of negative experiences.*
> *H5: MPVE will moderate the effect of permission justification on the privacy concerns, such that the effect will be weaker for individuals with high levels of negative experiences.*
> *H6: MPVE will moderate the effect of the perceived app popularity on the privacy concerns, such that the effect will be weaker for individuals with high levels of negative experiences.*

Following the privacy calculus, *download intentions* are influenced by a trade-off between benefits and costs which individuals face (Dinev et al. 2006). Besides an indicator of trustworthiness, *app popularity* can also indicate product attractiveness (Duan et al. 2009) and, therefore, can be seen as a benefit of downloading an app:

> *H7: Perceived app popularity positively influences the intention to download the MAR app.*

Our newly introduced variable *attitudes towards AR* captures individuals' overall attitudes towards AR. The higher the measure, the more positive the attitudes. We argue that the overall attitudes are directly influenced by specific privacy concerns related to our hypothetical MAR app. This follows our claim that

MAR as a type of AR technology will strongly influence individuals' overall attitudes towards the technology as a whole. We control for whether participants know what AR is and which mockup they saw before (the one without mentioning AR or the one with AR). Thus, we hypothesize:

> *H8: Privacy concerns related to the MAR app negatively influence the attitudes towards augmented reality in general.*

In turn, if individuals have positive attitudes towards AR, they will be more likely to download an MAR app and the fact that the app has the AR functionality will be seen as a benefit in the privacy calculus trade-off:

> *H9: The attitudes towards augmented reality in general positively influence the intention to download the MAR app.*

Prior literature indicates that privacy risks can be seen as the associated costs in the privacy calculus (Keith et al. 2013). Thus, such risks and related concerns might negatively affect the intentions:

> *H10: Users' privacy concerns related to the MAR app negatively influence their intention to download this app.*

Figure 1 shows the resulting research model with the hypotheses.

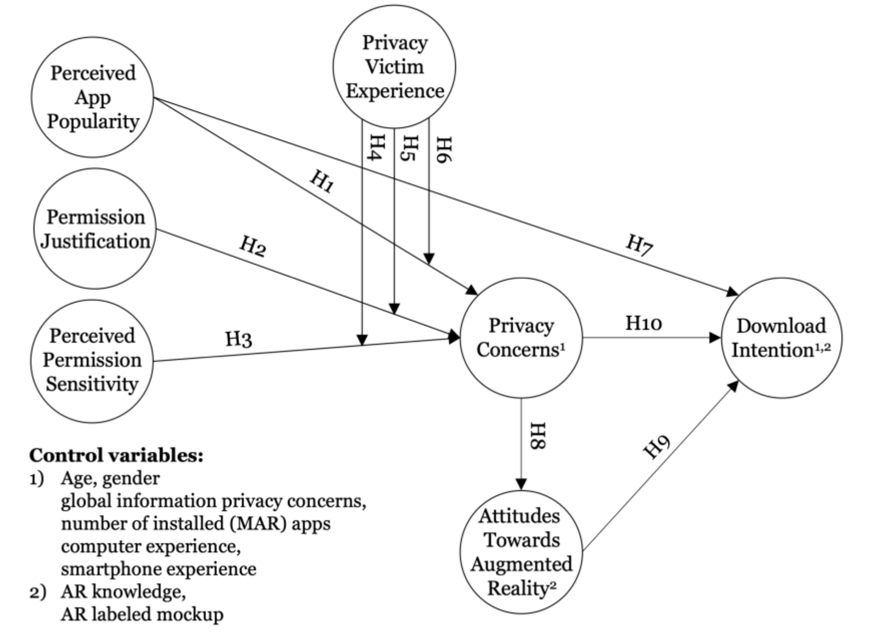

Figure 1. Research Model

Data Collection and Initial Sample

Since the study was conducted in Germany, we had to translate the items into the aforementioned language of the participants. We checked for equivalence with five research colleagues. The questionnaire items can be found in the appendix. We recruited participants via social media platforms (LinkedIn, Facebook, Xing) in specialized groups for AR or app development and in forums. Participants could win one of five Amazon vouchers worth 20€ each. 173 participants started the survey and 102 completed it. Ten participants answered a test question wrong and were discarded. One participant was deleted since she/he stated not to own a smartphone. Thus, our sample contains 91 valid answers. The median age of the participants is 24 years (minimum 19 years, maximum 61 years). There are 40 males and 51 females in the sample. The majority of the participants (63.74%) have A levels degrees, followed by 15.38% and 10.99% of the participants who hold a bachelor's and master's degree, respectively.

Results

This section presents the preliminary results for the initial sample. We tested the model using SmartPLS version 3.2.8 (Ringle et al. 2015). Since our research goal is to predict the target constructs *privacy concerns* and *download intention*, we use PLS-SEM for our analysis instead of CB-SEM which is generally used for theory testing (Hair et al. 2011). For the PLS algorithm, we choose the path weighting scheme with a maximum of 300 iterations and a stop criterion of 10^{-7}. For the bootstrapping procedure, we use 5000 bootstrap subsamples and no sign changes as the method for handling sign changes during the iterations of the bootstrapping procedure.

As the model is measured reflectively, we need to evaluate its internal consistency reliability, convergent validity and discriminant validity to assess the constructs properly (Hair et al. 2011). By following these steps, we are able to assess our constructs and preliminarily test our model hypotheses. Internal consistency reliability (ICR) is assessed by calculating Cronbach's α and the composite reliability. The values of both measures should be between 0.7 and 0.95 for research that builds upon accepted models. Table 1 shows the results for the two measures. The only problematic value is the one for the control variable global information privacy concerns (GIPC). Here, we also had to drop item 1 with a loading of 0.168. However, the composite reliability is acceptable and the loadings are between -0.626 (item 4 is a reverse item) and 0.837 with an average variance extracted (AVE) larger than 0.5. Assessing the AVE is part of checking the convergent validity. Convergent validity is given if the outer loadings are larger than 0.7 and the AVE is larger than 0.5. Due to space limitations we do not report outer loadings and cross-loadings of the constructs. The only items below 0.7 are item 2 of *perceived app popularity* (0.609), item 3 of *download intention* (0.593) and item 4 of *GIPC*. As for GIPC, the AVE is still larger than 0.5 with these items. Thus, we refrained from deleting them. Lastly, we assess the discriminant validity, i.e. the degree of uniqueness of a construct compared to other constructs (Hair et al. 2011). We assess the cross-loadings and find that all outer loadings of a given construct are larger than its cross-loadings with other constructs. In addition, we apply the Fornell-Larcker criterion comparing the square root of the constructs' AVE with the correlations with other constructs. The square root of the AVE of each of our constructs is larger than the correlation with other constructs. Thus, discriminant validity is established.

Construct	**Cronbach's α**	**Comp. reliability**	**AVE**
Perceived permission sensitivity	0.871	0.920	0.794
Perceived app popularity	0.887	0.829	0.628
Privacy concerns	0.897	0.929	0.765
Attitudes towards AR	0.898	0.928	0.764
Download Intention	0.785	0.871	0.701
GIPC	0.571	0.733	0.558

Table 1. ICR and AVE of reflective constructs

We assess collinearity and the path coefficients in this section. Collinearity seems to not be an issue in our model with a maximum inner VIF value equal to 1.712. The results for the path coefficients of the structural model can be found in Table 2. Statistical significance is indicated by asterisks, ranging from three asterisks for p-values smaller than 0.001 to one asterisk for p-values smaller than 0.05.

The results indicate that hypotheses 3, 8, 9, 10 can be confirmed. The perceived permission sensitivity has a strong positive effect on privacy concerns. Besides that, privacy concerns are only influenced by mobile privacy victim experience (positive effect) and the control variable GIPC. In addition, the moderated relationship of permission sensitivity and privacy victim experience is statistically significant but negative, indicating that more negative experiences would alleviate the effect of perceived permission sensitivity. Thus, hypotheses 4 cannot be confirmed. This is an interesting finding for further investigations in our research process. As hypothesized in H8, privacy concerns related to our MAR app seem to negatively influence the overall attitude towards AR. The effects related to download intention as a dependent variable are only partly statistically significant, i.e. attitudes towards AR have a positive effect and privacy concerns have a negative effect. However, perceived app popularity is not statistically significant.

DV: Privacy Concerns	**Path Coefficients and Significance Level**	**DV: Download Intentions**	**Path Coefficients and Significance Level**
R^2	0.603	R^2	0.440
Adjusted R^2	0.530	Adjusted R^2	0.353
Perceived permission sensitivity (PS)	0.510***	Perceived app popularity (PAP)	0.112
Permission justification (PJ)	-0.015	Attitudes towards AR	0.237*
Perceived app popularity (PAP)	-0.076	Privacy concerns	-0.362***
Mobile Privacy victim experience (MPVE)	0.175*	**DV: Attitudes towards AR**	
PS*MPVE	-0.234**	R^2	0.068
PJ*MPVE	-0.011	Adjusted R^2	0.036
PAP*MPVE	0.016	Privacy concerns	-0.217*
GIPC	0.221*		

Table 2. Structural Model Results (only statistically significant controls shown)

Limitations and Further Steps

The limitations of this short paper are related to the small and not representative sample. However, we argue that the sample is large enough for this pretest to give an insight into the used instruments and the experiment design, and possibly change certain elements accordingly. In addition, there are potential self-report biases (e.g. social desirability). We addressed this issue by gathering the data fully anonymized.

In this short paper, we showed our current progress in investigating privacy concerns and attitudes related to MAR applications. We outlined our current research design and presented preliminary results to validate the used constructs. We will refine our research design in the next four months and plan to gather answers of 1,000 smartphone users in Germany with the help of a market research company. Thereby, we ensure sufficiently large sub-groups for the vignette-based experiment design. Based on our preliminary results, we argue that there are other relevant variables to be included in the final model. For example, it is interesting to investigate whether users associate less strict data protection practices with free apps compared to paid apps (Han et al. 2019). Thus, the effect of a monetary cue could potentially influence the privacy concerns. In addition to privacy concerns, we plan to include a context-specific trust concept (in the app developer) in the model in order to account for the rationale that trust can serve as a mediator between privacy concerns and intentions (Smith et al. 2011). Upon completion, we hope that the study provides insights for the underexplored area related to user perceptions about MAR applications with a special focus on privacy concerns and the role of preexisting attitudes related to AR. Furthermore, we want to provide guidance for MAR developers with respect to permission design and transparency.

References

All websites last accessed August 21, 2019.

Ackerman, M. S., and Mainwaring, S. D. 2005. "Privacy Issues and Human-Computer Interaction," in *Security and Usability: Designing Secure Systems That People Can Use*, S. Garfinkel and L. Cranor (eds.), O'Reilly, Sebastopol, CA, pp. 381–400.

Android Developers. 2019. "Android Permissions Overview." (https://developer.android.com/guide/topics/permissions/overview#permission-groups).

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339–370.

Apple. 2019. "Apple Measure App." (https://support.apple.com/en-us/HT208924).

Azuma, R. T., Baillot, Y., Feiner, S., Julier, S., Behringer, R., and Macintyre, B. 2001. “Recent Advances in Augmented Reality,” in *IEEE Computer Graphics And Applications*, pp. 34–47.

Bansal, G., Zahedi, F. M., and Gefen, D. 2010. “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online,” *Decision Support Systems* (49:2), Elsevier B.V., pp. 138–150.

Bhattacherjee, A., and Sanford, C. 2006. “Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model,” *Management Information Systems Quarterly* (30:4), pp. 805–825.

Chen, R., and Sharma, S. K. 2015. “Learning and Self-Disclosure Behavior on Social Networking Sites: The Case of Facebook Users,” *European Journal of Information Systems* (24:1), pp. 93–106.

Cook, T. 2016. “Apple CEO Tim Cook Thinks Augmented Reality Will Be as Important as ‘Eating Three Meals a Day,’” *Interview Utah Tech Tour, Accessed via Business Insider*. (http://www.businessinsider.com/apple-ceo-tim-cook-explains-augmented-reality-2016-10?r=US&IR=T).

De Cristofaro, E. 2011. “Reclaiming Privacy for Smartphone Apps,” in *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 84–92.

Dacko, S. G. 2017. “Enabling Smart Retail Settings via Mobile Augmented Reality Shopping Apps,” *Technological Forecasting and Social Change* (124), Elsevier Inc., pp. 243–256.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. “Privacy Calculus Model in E-Commerce - a Study of Italy and the United States,” *EJIS* (15:4), pp. 389–402.

Duan, W., Gu, B., and Whinston, A. B. 2009. “Informational Cascades and Software Adoption on the Internet: An Empirical Investigation,” *MIS Quarterly* (33:1), pp. 23–48.

Felt, A. P., Egelman, S., and Wagner, D. 2012. “I’ve Got 99 Problems, but Vibration Ain’t One: A Survey of Smartphone Users’ Concerns,” in ACM *SPSM 12 Proceedings*, pp. 33–44.

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., and Ling, H. 2017. “Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective,” *Decision Support Systems* (94), pp. 19–28.

de Guzman, J. A., Thilakarathna, K., and Seneviratne, A. 2018. “Security and Privacy Approaches in Mixed Reality: A Literature Survey.” (https://doi.org/arXiv:1802.05797v2).

Hair, J., Ringle, C. M., and Sarstedt, M. 2011. “PLS-SEM: Indeed a Silver Bullet,” *The Journal of Marketing Theory and Practice* (19:2), pp. 139–152.

Han, C., Reyes, I., Elazari, A., On, B., Reardon, J., Feal, Á., Bamberger, K. A., Egelman, S., and Vallina-rodriguez, N. 2019. “Do You Get What You Pay For? Comparing The Privacy Behaviors of Free vs. Paid Apps,” in *Workshop on Technology and Consumer Protection (ConPro ’19)*, pp. 1–7.

Harborth, D. 2017. “Augmented Reality in Information Systems Research: A Systematic Literature Review,” in *Twenty-Third Americas Conference on Information Systems (AMCIS)*, pp. 1–10.

Harborth, D. 2019. “Unfolding Concerns about Augmented Reality Technologies: A Qualitative Analysis of User Perceptions,” in *Wirtschaftsinformatik (WI19)*, pp. 1262–1276.

Harborth, D., Hatamian, M., Tesfay, W. B., and Rannenberg, K. 2019. “A Two-Pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality Applications,” in *Hawaii International Conference on System Sciences (HICSS) Proceedings*, pp. 5029–5038.

Harborth, D., and Pape, S. 2018. “Privacy Concerns and Behavior of Pokémon Go Players in Germany,” in *Privacy and Identity Management. The Smart Revolution. IFIP Advances in ICT, Vol 526*, M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner (eds.), Springer, Cham, pp. 314–329.

Hatamian, M., Serna, J., Rannenberg, K., and Igler, B. 2017. “FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps,” in *TrustBus 2017 Proceedings*, pp. 1–16.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. “Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior,” *International Journal of Human Computer Studies* (71:12), Elsevier, pp. 1163–1173.

Kelley, P. G., Cranor, L. F., and Sadeh, N. 2013. “Privacy as Part of the App Decision-Making Process,” *CHI ’13 Proceedings*, pp. 3393–3402.

Kohn, V., and Harborth, D. 2018. “AUGMENTED REALITY – A GAME CHANGING TECHNOLOGY FOR MANUFACTURING PROCESSES?,” in *ECIS2018 Proceedings*, Portsmouth, UK, pp. 1–19.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336–355.

Microsoft. 2017. “Microsoft HoloLens.” (https://www.microsoft.com/microsoft-hololens/en-us/buy).

Mylonas, A., Kastania, A., and Gritzalis, D. 2013. “Delegate the Smartphone User Security Awareness,” *Computers & Security* (34), pp. 47–66.

Nellis, S. 2017. “Google, Apple Face off over Augmented Reality Technology,” *Reuters*. (https://www.reuters.com/article/us-google-apple/google-apple-face-off-over-augmented-reality-technology-idUSKCN1BA001).

Nicas, J., and Zakrzewski, C. 2016. "Augmented Reality Gets Boost From Success of 'Pokémon Go,'" *Wall Street Journal*. (https://www.wsj.com/articles/augmented-reality-gets-boost-from-success-of-pokemon-go-1468402203).

Painter, M. 2013. "Fortify on Demand Mobile Releases the HP Mobile Apps Security Vulnerability Report," *HP Official Website*. (http://www.www8-hp.com/emea_africa/fr/hp-news/press-release.html?id=1528865#.XMjFIS-B3p4).

Peterson, A. 2016. "Pokémon Go Had 'full Access' to the Google Accounts of Some IPhone Players," *Washington Post*. (https://www.washingtonpost.com/news/the-switch/wp/2016/07/12/pokemon-go-had-full-access-to-the-google-accounts-of-some-iphone-players/).

Petty, R. E., Cacioppo, J. T., and Schumann, D. 1983. "Central and Peripheral Routes to Advertising Effectiveness: The Moderating Role of Involvement," *JCR* (10:2), pp. 135–146.

Rauschnabel, P. A., He, J., and Ro, Y. K. 2018. "Antecedents to the Adoption of Augmented Reality Smart Glasses: A Closer Look at Privacy Risks," *Journal of Business Research* (92), Elsevier, pp. 374–384.

Ringle, C. M., Wende, S., and Becker, J. M. 2015. *SmartPLS 3*, Boenningstedt: SmartPLS GmbH, http://www.smartpls.com. (http://www.smartpls.com).

Simnett, J. 2018. "Mergers And Acquisitions In The AR/VR Sector: Time For Brands To Engage?," *Brand Quarterly*. (www.brandquarterly.com/mergers-acquisitions-arvr-sector-time-brands-engage).

Slyke, C. V., Johnson, R., Jiang, J., and Shim, J. T. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp. 415–444.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Theory and Review Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1015.

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

Appendix - Questionnaire Items

All items are measured on a 7-point Likert scale, if not otherwise indicated.

Perceived Permission Sensitivity (Gu et al. 2017)
1. Measure it! requests many permissions.
2. Measure it! requests sensitive permissions.
3. The potential risk related to the permission requests of Measure it! is high.

Privacy Concerns (Gu et al. 2017)
1. I think Measure it! will over-collect my personal information.
2. I will worry that Measure it! leaks my personal information to irrelevant third-parties.
3. If I were to download and use this app, I would be concerned that Measure it! would violate my privacy.
4. If I were to download and use this app, I would be concerned that Measure it! would misuse my personal information.

Overall Preexisting Attitude Towards Augmented Reality (Chen and Sharma 2015)
Your overall attitude toward using Augmented Reality in general is:
1. Good
2. Beneficial
3. Positive
4. Favorable

Perceived App Popularity (Gu et al. 2017)
1. I think Measure it! is popular.
2. Measure it! is downloaded numerous times.
3. I think Measure it! is hot among users.

Download Intention (Gu et al. 2017)
1. I am willing to download Measure it!.
2. After reading the related information of Measure it!, I am willing to try Measure it!.
3. Based on the given information, I would prefer Measure it! over comparable apps.

(Mobile) Privacy Victim Experience (Malhotra et al. 2004)
How frequently have you personally been the victim of what you felt was an improper privacy invasion from your installed mobile apps? (1 = very infrequently; 7 = very frequently)

Demographics and Control Variables
Age, gender, computer experience, smartphone experience, number of installed apps, number of installed MAR apps, global information privacy concerns (GIPC) (Malhotra et al. 2004; Smith et al. 1996) (item 1 dropped), knowledge about AR