Privacy Concerns and Behavior of Pokémon Go Players in Germany

David Harborth[0000-0001-9554-7567] and Sebastian Pape[0000-0002-0893-7856]

Chair of Mobile Business and Multilateral Security
Goethe University Frankfurt am Main
{david.harborth,sebastian.pape}@m-chair.de

Abstract. We investigate privacy concerns and the privacy behavior of users of the AR smartphone game Pokémon Go. Pokémon Go accesses several functionalities of the smartphone and, in turn, collects a plethora of data of its users. For assessing the privacy concerns, we conduct an online study in Germany with 683 users of the game. The results indicate that the majority of the active players are concerned about the privacy practices of companies. This result hints towards the existence of a cognitive dissonance, i.e. the privacy paradox. Since this result is common in the privacy literature, we complement the first study with a second one with 199 users, which aims to assess the behavior of users with regard to which measures they undertake for protecting their privacy. The results are highly mixed and dependent on the measure, i.e. relatively many participants use privacy-preserving measures when interacting with their smartphone. This implies that many users know about risks and might take actions to protect their privacy, but deliberately trade-off their information privacy for the utility generated by playing the game.

Keywords: privacy concerns, augmented reality, Pokémon Go, concerns for information privacy (CFIP), privacy calculus, privacy behavior

1 Introduction

The location-based augmented reality (AR) smartphone game Pokémon Go (cf. Fig. 1) is amongst the most successful smartphone applications of all time and led to a major increase in public awareness about AR [26, 32]. The game has broken several records [44] and it was shown that its users develop a strong attachment to the game [30]. Pokémon Go poses relatively strong privacy threats compared to other smartphone applications, due to the AR functionalities and the location-based nature. There is almost no research on privacy issues with regard to AR technologies [21]. Thus, we investigate privacy concerns about organizational information privacy practices and privacy-related behaviors of active Pokémon Go players in Germany. Three research questions arise: First, are privacy concerns a relevant issue for Pokémon Go players and do they differ in magnitude between different groups of players? Second, is there a relationship between the different dimensions of privacy concerns and the actual use behavior? Third, what are active players doing to protect their privacy on their smartphone?

Fig. 1: Pokémon Go on iOS [5]

The success of Pokémon Go [50] allows it to address these questions for an AR technology based on a large scale user study for the first time. Understanding the heterogeneous perceptions on privacy is necessary since many experts predict that AR will become one of the next big technological innovations with a massive market potential [8, 25]. Privacy aspects are especially important for AR because of its pervasiveness associated the advancements of wearable AR technologies (e.g. head-mounted displays). This leads to a situation where the user is continuously provided with context-sensitive information about her or his environment [19]. This, in turn, makes it necessary to continuously gather and process all kinds of data. Privacy violations can happen to actual users of a system – due to the increasing collection of several different data types [25] – or to the users' direct environment. The case of the social environment could be observed in the past for Google Glasses with several reports about angry civilians who had the feeling of being filmed by the wearer and bars which prohibited entry when wearing the glasses. This partly led to the failure of the device in the consumer market [49]. This case emphasizes the need to understand privacy concerns and behaviors of users in respect to AR technology even more. We investigate the privacy concerns based on a sample of 683 active players of Pokémon Go in Germany. The results indicate that privacy concerns are relatively strong throughout different demographic groups (cf. Table 1). This is a surprising result, considering that the participants are all active players of the game. Thus, in the second stage of the research, a second online survey with 199 participants is conducted to figure out specific measures how players protect their privacy.

The remainder of the paper is structured as follows. A brief background on Pokémon Go, AR and related work on privacy is given in Sect. 2. The methodology is described in Sect. 3 and the results are presented in Sect. 4. In Sect. 5 results and their limitations are discussed. Section 6 concludes this work.

2 Theoretical Background

In the following part, we provide theoretical background on Pokémon Go, augmented reality and the current literature on privacy.

2.1 Pokémon Go and Augmented Reality

Pokémon Go [3] is a location-based augmented reality (AR) smartphone game developed by Niantic, a former Google owned company [3, 31]. Many people see Pokémon Go as the unofficial successor of Ingress [2], another location-based smartphone game, also developed by Niantic. Up to now, no homogeneous opinion, of whether Pokémon Go matches all criteria of AR is formed. However, there is broad agreement that it is a first important step towards AR [17, 20, 27, 28]. Thus, we approach Pokémon Go as an AR application for the course of our research.

AR is defined in multiple ways, whereas the definition by Azuma et al. [4, p. 34] provides a comprehensive understanding of the technology. They define AR in a way that "[...] an AR system [...] 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". The differentiation towards virtual reality (VR) is currently not always done in the public discussion. Milgram et al. [29] illustrate the dimensions of mixed reality (MR) based on a x-axis (cf. Fig. 2). Based on this, it is important to distinguish whether the environment is real (AR) or virtual (VR). Up to now, research on AR mainly focused on technical aspects and not on the user behavior [21, 43]. Since AR is expected to be one of the upcoming technologies [8], it is important to investigate user behavior and privacy issues.

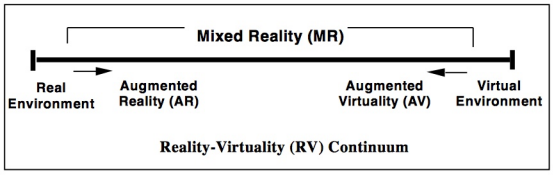

Fig. 2: The Reality-Virtuality Continuum [29]

2.2 Privacy and the Privacy Paradox

The definition of privacy in the literature consists of a variety of different perspectives [6, 39]. An often cited definition is given by Warren and Brandeis in 1890. They say that privacy is "the right to be left alone" [48]. In the context of this paper, the privacy definition provided by Culnan [10, p. 344] is used, where "privacy is the ability of an individual to control the access others have to personal information". The notion of control plays a crucial role in the privacy literature [7] and for the concerns about organizational practices. Thus, we choose this definition for our research context. Previous literature shows that privacy concerns play an important role for the usage of internet services. For example, Tang et al. [45] argue that retailers can improve privacy and trust if they send clear signals that they will protect the privacy of the customers. Culnan and Armstrong [11, p. 107] provide a framework where users provide their personal data willingly, if they perceive the firm's information processes as "fair". Fair means in this context that these processes "provide individuals with control over

the disclosure and subsequent use of their personal information". Differences in privacy behavior with regard to demographics [10, 11, 38, 46] and cultural differences [14] are investigated in previous literature as well. But it is shown that the majority of literature focuses on student samples based in the United States [6]. In summary, it can be stated that privacy plays an important role for the usage of online services. However, it is important to mention that "privacy concern is only one of a number of factors affecting Internet and e-services use" [16, p. 51].

Closely related to the discussion on privacy concerns and behavior is the so called "privacy paradox". This phenomenon describes the divergence of the actual behavior of users compared to the stated attitudes when dealing with privacy issues [1, 9, 33, 41]. The privacy paradox is a well-known topic in information systems research. Spiekermann et al. [41] experimentally show that participants reveal a multitude of information, which enables providers to construct a detailed profile during an online-shopping tour, although they stated to be concerned about their privacy before the experiment. The paper by Berendt et al. [9] is built on the previously mentioned paper and shows the existence of the privacy paradox by using an e-commerce experiment, too. Acquisti and Grossklags present another point of view on the privacy paradox. They show that while people have high standards regarding their privacy attitudes, their decision process is influenced by psychological factors like "incomplete information, bounded rationality and systematic psychological deviations from rationality" [1, p. 29]. These limitations lead to a trade-off of "long-term privacy for short-term benefits" [1, p. 24]. Norberg et al. [33] investigate why this divergence of actual behavior and attitudes towards privacy exists. The results support the hypothesis that risk perceptions of users when disclosing personal information influence the intentions to provide personal information. However, the second hypothesis about the effect of trust on the disclosure behavior could not be confirmed.

In summary, it is important to recognize that people do not always behave in the way they state that they would do. Therefore, all results that deal with attitudes of users, in particular regarding to privacy, have to be treated with caution if the goal of the research is to make valid statements for decision choices. Thus, we include the second survey on the actual privacy measures in this work.

3 Methodology

The methodology presents the design and data collection of the first and the second survey. The second survey on actual privacy related behavior was conducted after we conducted the first one on privacy concerns.

3.1 Questionnaire

Survey I We conducted the study with a German panel, thus all items had to be translated into German. As we wanted to ensure content validity of the translation, we followed a rigorous translation process [47]. First, the English questionnaire was translated into German with by a certified translator (translators are standardized

following the DIN EN 15038 norm). Afterwards, the German version was given to a second independent certified translator who retranslated the questionnaire to English. This step was done to ensure the equivalence of the translation. Third, a group of five academic colleagues checked the two English versions with regard to this equivalence. All items were found to be equivalent. In a last step, the German version of the questionnaire was administered to students of a Masters course to check preliminary reliability and validity.

Privacy concerns with regard to organizational information privacy practices are represented by the variables pcollection, errors, unauthorized secondary use and improper access. As these variables cannot be measured directly (latent variables), they have to be operationalized in order to quantify the concerns via a user study. We choose the privacy constructs by Smith et al. [40], as they are widely tested with regard to validity and reliability (cf. Stewart and Segars [42]). The constructs are built by calculating mean sum scores of the single items belonging to the respective construct (cf. Appendix A). *Collection* is defined as the concern of people that too much data about them is collected over time. *Errors* represent users' concerns about inaccurate or false personal data in databases. *Unauthorized secondary use* measures the concern that personal data is used for another purpose than initially disclosed without the user's authorization. *Improper access* captures concerns about unauthorized people having access to the user's personal data [40, p. 172].

Survey II The questionnaire of the second survey covers questions about actual privacy protecting measures, which active Pokémon Go players undertake. The questionnaire contains the same demographic questions about age, gender, education and smartphone experience, as well as actual use behavior of Pokémon Go as the first survey. The steps are derived from internet search [18], as well as valuable feedback from colleagues. Measure 1 (M1) asks about whether users turn off services that potentially collect location data. Measure 2 (M2) deals with the use of a separate e-mail address used only for games. Measure 3 (M3) specifies this furthermore and asks about the use of different e-mail addresses for games and social network sites (sns). Measure 4 (M4) asks the participants whether they review which applications can access other accounts (e.g. Facebook). Measure 5 (M5) asks whether users reset the advertising ID on their phone and measure 6 (M6) deals the camera access rights of Pokémon Go. All measures are formulated as statements and could be answered with "yes", "no", "sometimes" or "I don't know". The specific questions can be found in Appendix B.

3.2 Data Collection

Survey I In order to ensure high quality of the sample, a certified sample provider (certified with ISO 26362 norm) was employed to get access to their online panel for Germany. By focusing on German users of the game, we could address two potential problems. First, country-specific differences in privacy concerns are eliminated and controlled. Second, by focusing on one country, we could gather a relatively large data set. The survey itself was administered with LimeSurvey

(version 2.63.1) [37]. The panel provider distributed the survey's link to 9338 participants until the aimed sample size of active players was reached. Of 9338 approached participants, 683 active Pokémon Go players remained, excluding participants who dropped out due to wrong answers to test questions and age restrictions (data was only collected for at least 18 year old participants). Table 1 presents summary statistics for this data set. Further information with regard to the demographics can be found in the paper by Harborth and Pape [22].

Survey II Since of the constructs in Survey I only provide information about attitudes and stated concerns, we wanted to consider actual use behavior with regard to privacy protecting measures. Because of anonymized answers in Survey I, we could not ask the same participants. In addition, we could not employ a panel provider as in Survey I due to limited resources. Thus, we created a very brief questionnaire (see Sect. 3.1) and administered it with LimeSurvey (version 2.63.1) [37]. We distributed the link of the online survey in three Pokémon Go Facebook groups (Germany, Frankfurt and Munich). All groups are closed groups with approximately 30,000 members altogether. The questionnaire was online for 4 days and 238 users started it, whereas only 200 participants finished it. One participant's answers were deleted, because he or she stated to be younger than 18 years. Table 2 presents the summary statistics for this data set.

3.3 Demographics

Survey I Table 1 shows that the median age is 32 years and that there is a larger share of women than men in the sample. Furthermore, the secondary school leaving certificate[1] and the A levels certificate[2] are the most common educational qualifications. With regard to these demographics, it can be argued that this data set represents the German population to an acceptable degree. The smartphone experience has a median of 6 years. The privacy constructs have all at least a median value of 5.5, implying that most players agree to the statements made in the constructs' items. The actual use frequency has a median of 5 which stands for playing "several times a week". Improper access has a median of 6.333.[3]

Survey II The demographics of the second survey are slightly different to the first survey with regard to age, gender and smartphone experience (cf. Table 2). The participants of the second survey are 6 years younger with regard to the median age and there are slightly more men than women in Survey II. The users in Survey II have one year more smartphone experience. Although the users in both surveys say that they are active Pokémon Go players, the participants in Survey II state that they play Pokémon Go several times a day (median of 7) and players of Survey I state that they play it only several times a week.

[1] German: "Realschulabschluss"
[2] German: "Abitur"
[3] This is possible because of the construct is calculated based on the mean sum score of three items (the other three concern constructs each consist of four items).

Table 1: Descriptive Statistics Survey I (N=683)

	Mean	Median	Std. Dev.	Min.	Max.
Age	34.539	32	(11.531)	18	66
Gender	0.572	1	(0.495)	0	1
Educational Qualification	3.977	4	(1.207)	1	7
Smartphone Experience	5.958	6	(2.359)	0	10
Collection	5.349	5.5	(1.172)	1	7
Errors	5.355	5.5	(1.198)	1	7
Unauthorized Secondary Use	6.015	6.5	(1.071)	1	7
Improper Access	5.971	6.333	(1.090)	1	7
Frequency of Actual Use	5.517	5	(1.619)	1	10

Apparently, the participants acquired through Facebook groups are rather heavy users compared to the ones acquired with the help of a sample provider. A self-selection mechanism could explain this difference. In these Facebook groups, players exchange information about new offers, versions and places to hunt for special Pokémons. This is especially interesting for highly attached players, which would indicate that those are rather heavy users.

Table 2: Descriptive Statistics Survey II (N=199)

	Mean	Median	Std. Dev.	Min.	Max.
Age	28.884	26	(8.695)	18	58
Gender	0.477	0	(0.501)	0	1
Educational Qualification	4.261	4	(1.142)	1	7
Smartphone Experience	7.156	7	(2.279)	2	11
M1	2.050	2	(0.827)	1	4
M2	1.658	2	(0.654)	1	3
M3	1.668	2	(0.689)	1	3
M4	1.563	1	(0.838)	1	3
M5	2.221	2	(0.652)	1	4
M6	1.492	1	(0.658)	1	3
Frequency of Actual Use	6.729	7	(1.783)	1	10

4 Results

We present the results of Survey I and Survey II in the following sections.

4.1 Survey I - Privacy Concerns

The variables collection, errors, unauthorized secondary use and improper access are not normally distributed while actual use is normally distributed according to the Shapiro-Wilk test for normality. In the first part of the empirical assessment, it is investigated whether users' privacy concerns and the actual use behavior (i.e.

Table 3: Two-sample Wilcoxon rank-sum and two-sample t test (for actual use)

	Group Variables				
Variables	Age_{Median}	Age_{DN}	Gender	Education	Smartphone Exp.
Collection	z=-3.217**	z=-3.288**	n.s.	n.s.	n.s.
Errors	z=-6.644***	z=-5.852***	n.s.	z=2.766**	n.s.
Un. Sec. Use	n.s.	z=-3.020**	z=-4.019***	n.s.	n.s.
Imp. Access	z=-2.516**	z=-3.870***	z=-2.589***	n.s.	n.s.
Actual Use	n.s.	n.s.	n.s.	n.s.	t=-4.335***

t statistic for t test and z statistics for Wilcoxon rank-sum test
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

frequency of playing Pokémon Go) differ with regard to age, gender, education and smartphone experience. Therefore, categorical variables for group comparisons are created by dividing the scale of continuous variables into two meaningful groups. Categorical variables for group comparisons are created based on the variables age, smartphone experience and educational qualification. This is necessary because they are not binaries like gender. For creating a categorical variable, a threshold is needed that divides the scale into two meaningful groups.

The threshold for age is not clearly determinable because there are two rationales for dividing the data which are highly interesting to investigate in the context of privacy. The first approach is a median split, a commonly used technique for forming categorical variables in statistics [24]. This has the advantage of comparing two groups, similar in size, based on the actual median of the used data set. This results in the groups of participants aged 31 and younger and participants aged 32 and older. A categorical variable is created where 0 stands for participants aged 31 and younger and 1 for participants aged 32 and older. One group contains 341 participants and the second one 342. The second approach deals with the notion of "digital natives" (DN) versus "digital immigrants" (DI) [35]. Since there is a vivid discussion on whether the notion of DN is substantial [23], it is interesting in the context of privacy concerns to apply this threshold and investigate, whether it is true that DI are rather privacy sensitive and more concerned than the younger generation. A commonly named threshold for the oldest year of birth of a DN is 1980 [34]. The resulting two groups contain 446 entries for DN (37 years old and younger) and 237 entries for DI. The median split approach is applied for experience since this is the most meaningful approach, with groups with smartphone experience less than or equal to 5 years and greater than or equal to 6 years. Education is divided into a group with participants without university degree (NU), comprising all participants whose highest educational qualification is the German Abitur (N= 487) and a group with 196 participants holding at least a Bachelor's degree (U). Table 3 summarizes the results for the statistical assessment of whether the group differences in mean values are statistically significant or not.

For collection there are only significant differences for the two different age groups. Users' perceptions of the errors construct differs between younger and older participants as well as between participants without and with university

Table 4: Regression analysis of privacy concern variables and use behavior (N=683)

	(1)	(2)	(3)	(4)	(5)
	Dependent variable: actual use behavior				
Collection	0.0518				-0.00691
	(1.00)				(-0.11)
Errors		-0.0480			-0.170**
		(-0.91)			(-2.76)
Un. Sec. Use			0.124*		0.00368
			(2.05)		(0.03)
Imp. Access				0.149*	0.251*
				(2.53)	(2.19)
_cons	5.240***	5.774***	4.772***	4.630***	4.943***
	(18.70)	(20.00)	(12.85)	(13.01)	(12.78)

t statistics in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

degree. Interestingly, the group comparison of unauthorized secondary use is different for the age groups. For the median split, there is no statistically significant difference in the evaluation between younger and older players, whereas there is one for the case of DN versus DI. The evaluation for this construct differs significantly between women and men. For the improper access construct, statistically significant differences are prevalent for age and gender. The variable actual use is homogeneous across the different characteristics of Pokémon Go players except for smartphone experience. The question of whether privacy concerns influence the use behavior is addressed in the second part of the empirical analysis. Due to the breakdown into four variables, it is possible to assess which kind of privacy concern exerts what kind of influence on use behavior. This question is addressed with a two-stage process (cf. Table 4). First, each privacy concern variable is treated as the independent variable in a simple linear regression model, with actual use behavior as the dependent variable. Second, a multiple regression model, containing all independent variables, is calculated in order to assess the effect of the different dimensions of privacy concerns on use behavior simultaneously.
The results of the regression analysis indicate that privacy concerns have no significant impact on the actual use behavior. Although there are statistically significant relationships, the effect sizes are rather small and therefore not relevant.

In summary, the results about privacy concerns indicate that there are significant differences in the different dimensions of concerns between younger and older players. Furthermore, gender matters for two of the four dimensions. An additional regression analysis with the actual use frequency revealed no clear impact of privacy concerns, indicating that players might well be aware of privacy dangers and are concerned about it, but are still playing the game. Thus, although privacy is perceived as important, it does not affect the use of Pokémon Go. The game requires several more types of data compared to other smartphone applications due to its location-based and AR nature. This contrary result could be a case of the privacy paradox [33], where people state that privacy is important for them, but act in the opposite way.

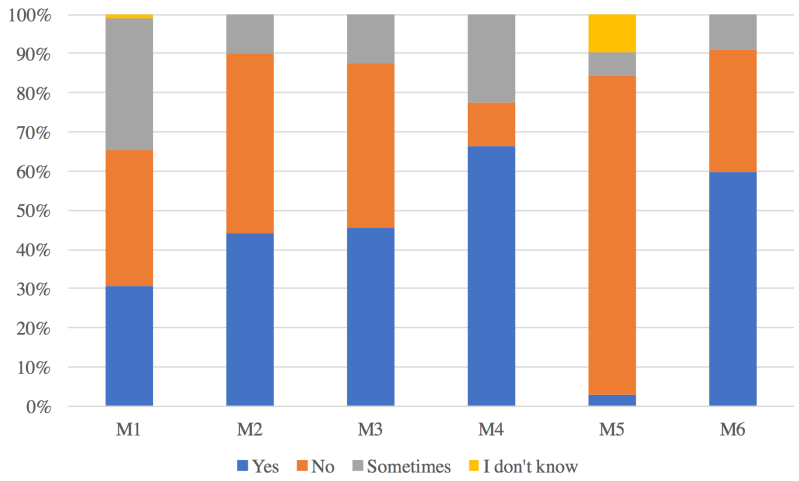

Fig. 3: Relative frequency of the measures taken by Pokémon Go players

4.2 Survey II - Privacy Behavior

The distribution of the answers on the privacy protecting measures are illustrated in Fig. 3. The number of participants who turn off services that collect location data is approximately the same as those who do not and those who sometimes do it. 45% of the players use a separate e-mail address only for games and roughly the same number of players do not. The remaining users (10%) do it sometimes. The distribution for M3 (different e-mail addresses for games and sns) is almost the same as for M2. Interestingly, more than 65% of the Pokémon Go players review the access of applications to other accounts and only 10% do not. The remaining users undertake this measure sometimes. More than 80% of the users do not reset the advertising ID and only 10% do know about it at all. The majority of the players forbid Pokémon Go the camera access (60%) and 10% do it somestimes. The remaining participants do not forbid it.

5 Discussion

After we discussed the results of the two surveys independently of each other, we combine and interpret our results in the following part. After that, we discuss the limitations of our work.

5.1 Interpretation and Implications of the Results

As mentioned previously, there are significant differences in the different dimensions of the concerns between younger and older players. Furthermore, gender matters for two of the four dimensions. Gender differences in privacy concerns were also shown to be prevalent in past literature (e.g. [38, 46]). For the age differences, the results indicate that relatively older players of Pokémon Go

are more concerned. This is in line with the dominant notion of less concerned younger internet users compared to older users with a higher awareness. The regression analyses do not show any impact of the privacy concern dimensions on the actual use behavior of Pokémon Go. Based on this, it can be said that concerns about the privacy practices of organizations exist amongst players of the game and that they are heterogeneous with regard to the certain demographic characteristics. However, these users still play a game, which has access to several data types and processes them. This behavior is in line with the notion of the privacy paradox. However, this explanation becomes inconclusive, when looking at the actual privacy preserving measures of the players. It can be seen that, depending on the measure, approximately half of the participants of the second survey engage regularly or sometimes in doing these measures. A combination of these results imply that the majority of Pokémon Go players are aware about the risks (since they actively try to preserve their privacy with the measures tested) and almost all players are concerned. However, it seems that playing the game provides so much utility that they willingly agree to the implicit trade-off between playing the game and loosing a certain degree of control over their privacy. This explanation for an opposing behavior with regard to information privacy is known as the privacy calculus [12, 13, 15]. The privacy calculus is often mentioned in the literature as an explanation for the privacy paradox.

5.2 Limitations

The main limitations concern the sample characteristics. Both samples contain relatively more younger Pokémon Go players. With respect to this, the sample is not representative for the German population. This skewness might also be caused by the fact that digital games are played rather by younger users than older ones. In addition, our survey is only conducted with German players. Thus, the results could possibly differ from surveys conducted in other countries or cultural regions. But, this focus brings along advantages for this research (cf. Sect. 3.2), which can outweigh the limitations. Another limitation relates to the German translation of the English constructs. The constructs might have been understood differently by the participants than originally intended. This is always a possible threat when adapting original constructs from a language to another. The last limitation emerges due to the fact of analyzing two different samples. As described in Sect. 3.2, we could not ask the same participants from the first survey about their privacy preserving measures. Therefore, we are not able to compare the relationship between concerns and actual privacy behavior on an individual level. In addition, it is possible that people lie about their actual behavior in surveys. Thus, asking people what they actually do is also prone to errors that can hardly be controlled for in an online survey.

6 Conclusion and Future Work

We contributed to the literature on privacy and augmented reality in several ways. First, we contributed to the body of literature on information privacy

by doing an empirical, not a normative work, that is based on a non-student sample with participants, who are not located in the United States [6,39]. Second, many studies on privacy only include perceptions and attitudes of users and no actual privacy-related behavior. By conducting the second survey, we are able to determine that relatively many Pokémon Go players act in a privacy-friendly way. By merging all the insights of both studies, we suggested that the majority of the Pokémon Go players are well aware of privacy risks and measures, but willingly trades-off benefits of the game against a higher level of privacy. Third, this research is one of the first to investigate privacy issues related to AR applications.

These insights indicate that users will abandon the protection of their privacy, if smartphone applications provide a level of utility that is high enough to outweigh the concerns. This conclusion is indepedent of the knowledge about and usage of privacy-preserving measures.

Future work should consider to include questions about privacy concerns and privacy measures in one questionnaire to include all three dimensions. First, the actual use behavior of the application. Second, the privacy concerns. Third, the actual privacy preserving measures undertaken by each participant (cf. Appendix B). In addition, our research on Pokémon Go and privacy could be conducted in other countries with different cultural values. This is especially interesting for the case of privacy perceptions and privacy preserving behavior. Another interesting dimensions is the investigation of this topic along different points in time. It could be investigated whether differences in the perception about Pokémon Go and associated privacy dimensions occur over time.

Acknowledgments

The authors wish to thank the Faculty of Economics and Business Administration of the Goethe University Frankfurt am Main for supporting this work with a grant within the funding program "Forschungstopf". This research was also partly funded by the German Federal Ministry of Education and Research (BMBF) with grant number: 16KIS0371. In addition, we would also like to thank Harald Zwingelberg for his valuable feedback with regard to the privacy measures.

References

1. A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, January/Fe(1):24–30, jan 2005.
2. Myk Gregory Albao. Ingress: A Game, Lifestyle and Social Network in One! http://www.wheninmanila.com/ingress-game-lifestyle-social-network/, 2014.
3. Apple App Store. Pokémon Go. https://itunes.apple.com/de/app/pokémon-go/id1094591345?mt=8%0A, 2017.
4. Ronald T. Azuma, Yohan Baillot, Steven Feiner, Simon Julier, Reinhold Behringer, and Blair Macintyre. Recent Advances in Augmented Reality. In *IEEE Computer Graphics And Applications*, number November/December, pages 34–47, 2001.
5. BBC. Pokemon and the power of nostalgia. http://www.bbc.com/news/world-asia-36780797, 2016.

6. France Bélanger and Robert E. Crossler. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4):1017–1041, 2011.
7. France Belanger, Janine S. Hiller, and Wanda J. Smith. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11(July 2016):245–270, 2002.
8. Heather Bellini, Wei Chen, Masaru Sugiyama, Marcus Shin, Shateel Alam, and Daiki Takayama. Virtual & Augmented Reality: Understanding the race for the next computing platform. Technical report, Goldman Sachs Equity Research, 2016.
9. Bettina Berendt, Oliver Guenther, and Sarah Spiekermann. Privacy in e-commerce. *Communications of the ACM*, 48(4):101–106, apr 2005.
10. Mary J. Culnan. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly*, (September):341–364, 1993.
11. Mary J. Culnan and Pamela K. Armstrong. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1):104–115, feb 1999.
12. Tobias Dienlin and Miriam J. Metzger. An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21(5):368–383, 2016.
13. Tobias Dienlin and Sabine Trepte. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3):285–297, 2015.
14. Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management*, 14(4):57–93, 2006.
15. Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80, 2006.
16. Tamara Dinev and Paul Hart. Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. *e-Service Journal*, 4(3):25–60, 2006.
17. Ian Evans. Pokémon Go May Not Truly Be Augmented Reality, and That's OK. https://undark.org/2016/07/21/pokemon-go-isnt-augmented-reality-thats-okay/, 2016.
18. Bill Fitzgerald. Concrete Steps to Take to Minimize Risk While Playing Pokémon GO. https://funnymonkey.com/2016/concrete-steps-to-take-to-minimize-risk-while-playing-pokemon, 2016.
19. Jens Grubert, Tobias Langlotz, Stefanie Zollmann, and Holger Regenbrecht. Towards Pervasive Augmented Reality: Context-Awareness in Augmented Reality. *IEEE Transactions on Visualization and Computer Graphics*, PP(99):1–20, 2016.
20. Andy Gstoll. A love letter from augmented reality to Pokémon Go. https://thenextweb.com/insider/2016/08/19/augmented-reality-love-letter-pokemon-go/, aug 2016.
21. David Harborth. Augmented Reality in Information Systems Research: A Systematic Literature Review. In *Twenty-third Americas Conference on Information Systems*, pages 1–10, Boston, 2017.
22. David Harborth and Sebastian Pape. Exploring the Hype: Investigating Technology Acceptance Factors of Pokémon Go. In *2017 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, 2017.

23. Ellen Johanna Helsper and Rebecca Eynon. Digital natives: where is the evidence? *British Educational Research Journal*, 36(3):503–520, 2010.
24. Jörg Henseler and Georg Fassot. Testing Moderating Effects in PLS Path Models: An Illustration of Available Procedures. In Vincenzo Esposito Vinzi, Wynne W. Chin, Jörg Henseler, and Huiwen Wang, editors, *Handbook of Partial Least Squares*, chapter 30, pages 713–735. Springer, 2010.
25. Paul Hyman. Augmented-Reality Glasses Bring Cloud Security Into Sharp Focus. *Comm. of the ACM*, 56(6):18–20, 2013.
26. Ryan Kh. Augmented Reality Gets Boost From Pokemon Go. https://www.engadget.com/2016/09/28/augmented-reality-gets-boost-from-pokemon-go/, 2016.
27. Ben Lang. 'Pokémon Go' is Where I Draw the Line on "Augmented Reality". http://www.roadtovr.com/pokemon-go-is-where-i-draw-the-line-on-augmented-reality/, 2016.
28. Will Mason. Pokemon Go or: How I Learned To Stop Worrying About The Definition And Love Augmented Reality. https://uploadvr.com/pokemon-go-ar-definition/, 2016.
29. Paul Milgram, Haruo Takemura, Akira Utsumi, and Fumio Kishino. Augmented Reality: A class of displays on the reality-virtuality continuum. *SPIE Proceedings*, 2351(Telemanipulator and Telepresence Technologies):282–292, 1994.
30. Iva Nedelcheva. Analysis of Transmedia Storytelling in Pokémon GO. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 10(11), 2016.
31. Niantic Labs. Website of Niantic Labs. https://www.nianticlabs.com/, 2017.
32. Jack Nicas and Cat Zakrzewski. Augmented Reality Gets Boost From Success of Pokémon Go'. https://www.wsj.com/articles/augmented-reality-gets-boost-from-success-of-pokemon-go-1468402203, 2016.
33. Patricia A. Norberg, Daniel R. Horne, and David A. Horne. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1):100–126, jun 2007.
34. John Palfrey and Urs Gasser. *Born Digital: Understanding the First Generation of Digital Natives*, volume 13. Basic Books, 2008.
35. Marc Prensky. Digital Natives, Digital Immigrants. *On the Horizon*, 9(5):1–6, 2001.
36. L.D. Rosen, K. Whaling, L.M. Carrier, N.A. Cheever, and J. Rokkum. The Media and Technology Usage and Attitudes Scale: An empirical investigation. *Comput Human Behav.*, 29(6):2501–2511, 2013.
37. Carsten Schmitz. LimeSurvey Project Team. http://www.limesurvey.org, 2015.
38. Kim Bartel Sheehan. An Investigation of Gender Differences in Online Privacy Concerns and Resultant Behaviors. *Journal of Interactive Marketing*, 13(4):24–38, 1999.
39. H. Jeff Smith, Tamara Dinev, and Heng Xu. Theory and Review Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4):989–1015, 2011.
40. H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 20(2):167–196, 1996.
41. Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. In *EC '01 Third ACM Conference on Electronic Commerce*, pages 38–47, Tampa, FL, USA, 2001. Humboldt University Berlin, ACM.

42. Kathy A. Stewart and Albert H. Segars. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1):36–49, 2002.
43. J. Edward Swan II and J L Gabbard. Survey of User-Based Experimentation in Augmented Reality. In *1st International Conference on Virtual Reality*, pages 1–9, 2005.
44. Rachel Swatman. Pokémon Go catches five new world records. http://www.guinnessworldrecords.com/news/2016/8/pokemon-go-catches-five-world-records-439327, aug 2016.
45. Zhulei Tang, Yu Hu, and Michael D. Smith. Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4):153–173, apr 2008.
46. Markus Tschersich, Shinsaku Kiyomoto, Sebastian Pape, Toru Nakamura, Goekhan Bal, Haruo Takasaki, and Kai Rannenberg. On Gender Specific Perception of Data Sharing in Japan. In *31st IFIP TC 11 International Conference, SEC 2016*, pages 150–160, Ghent, Belgium, 2016.
47. Viswanath Venkatesh, James Thong, and Xin Xu. Consumer Acceptance and User of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, 36(1):157–178, 2012.
48. Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, IV(5):193–220, 1890.
49. Justin Burton Weidner. How & Why Google Glass Failed. http://www.investopedia.com/articles/investing/052115/how-why-google-glass-failed.asp, 2015.
50. Howard Yu. What Pokémon Go's Success Means for the Future of Augmented Reality. http://fortune.com/2016/07/23/pokemon-go-augmented-reality/, 2016.

All websites have been accessed last on July 20th, 2017.

A Questionnaire I

Collection
Coll1. It usually bothers me when companies ask me for personal information.
Coll2. When companies ask me for personal information, I sometimes think twice before providing it.
Coll3. It bothers me to give personal information to so many companies.
Coll4. I am concerned that companies are collecting too much personal information about me.
Errors
Err1. All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.
Err2. Companies should take more steps to make sure that the personal information in their files is accurate.
Err3. Companies should have better procedures to correct errors in personal information.
Err4. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Unauthorized Secondary Use
USU1. Companies should not use personal information for any purposes unless it has been authorized by the individuals who provided the information.
USU2. When people give personal information to a company for some reason, the company should never use the information for any other reason.
USU3. Companies should never sell the personal information in their computer databases to other companies.
USU4. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
Improper Access
IA1. Companies should devote more time and effort to preventing unauthorized access to personal information.
IA2. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.
IA3. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
Use Behavior
Please choose your usage frequency for Pokémon Go:

- Never
- Once a month
- Several times a month
- Once a week
- Several times a week
- Once a day
- Several times a day
- Once an hour
- Several times an hour
- All the time

The frequency scale is adapted from Rosen et al. [36]. All other items are measured with a seven-point Likert scale, ranging from "strongly disagree" (coded as 1) to "strongly agree" (coded as 7). Male participants are coded as 0 and females as 1.

B Questionnaire II

Which of the following options are you using while playing Pokmon Go?
M1. If possible, I turn off services that can be used to collect location data.
M2. I have a separate e-mail address, which I only use for games.
M3. I use different e-mail addresses for games and social networks.
M4. I review, which apps are authorized to access my other accounts (Twitter, Google, Facebook).
M5. I reset the advertising ID on my smartphone at least once per month.
M6. I forbid Pokémon Go to have access to my smartphone camera and use it without the Augmented Reality functionality.
The participants were able to answer the questions with "yes" (coded as 1), "no" (coded as 2), "sometimes" (coded as 3) and "I don't know" (coded as 4). In addition, the same questions as in Survey I were asked with regard to users' demographics and use behavior.

C Record of Changes According to the Reviews

1. All formal comments with regard to style, expression and typographical errors are revised.
2. Section 2.2 on the privacy definitions is shortened.
3. The relationship between the privacy paradox and the privacy calculus is clarified.
4. The methodological problems of doing a survey about behavior are elaborated in the section about limitations.
5. A more precise explanation for the demographic differences of privacy concerns is provided in Section 5.1.
6. The calculation of the median of the improper access construct is explained in more detail (commentary by the session chair during the Summer School)

D Response to Reviewer's Comments

Reviewer 1 Comment 1: Argumentation: See end section 2 (final paragraph). Is there a current breakdown or collapse of the highly theoretical notion of rationality (fact vs. fiction; people mis-representing what they do in polls to survey teams)? Does massive data collection simply expose to us more explicitly the lack of coherence between thought/action; intention/actual behaviour? Does it simply show that people air act with what ought to be a considerable amount of cognitive dissonance? Consider whether more could be made of these types of arguments.

Reply: We considered the reviewer's comment as an additional threat of validity and added "In addition, it is possible that people lie about their actual behavior in surveys. Thus, asking people what they actually do is also prone to errors that can hardly be controlled for in an online survey." in Section 5.2. (#4)

Reviewer 1 Comment 2: Explanation: Is the privacy paradox the same thing as the privacy calculus? If so, some clarification is needed.

Reply: No, they are not. However, we added further clarification to Section 2.2.

Reviewer 1 Comment 3: Is it companies or is it young people who do not care about privacy? Or both? Are there implications of the ways in which games, or addiction, or pleasure can all be used as a type of "Trojan horse" for weakening users commitment to privacy protection? On p2, while Google Glasses drew immediate attention to the aspects of privacy intrusion when filming, with the population at large mobile phones seemingly are not raising the same degree of concern: again, is this a backdoor trap into greater intrusion/monitoring/surveillance? Perhaps either the industrial designers/companies not thought through these difficulties or possibly the populations of their target markets (chiefly young peope) fundamentally do not care.

Reply: It's an interesting idea to investigate who causes the ignorance of privacy. However, this is beyond the scope of our work since we were only researching privacy concerns and intended behaviour of Pokémon Go players.

Reviewer 1 Comment 4: Survey: It is an interesting concept to bring a three-dimension survey together, but please explain what the methodological challenges are of undertaking a survey about behaviour.

Reply: Even if you ask directly for the actual behavior, there is always a possibility that participants lie in the survey. This limitation cannot be resolved, unless you observe people in the field. We added this limitation in Section 5.2. (#4)

Reviewer 1 Comment 5: Findings: The findings (e.g., in section 5.1) appear to be quite important, BUT their precise implications do not appear to be explored in detail (p11): "there are significant differences in the different dimensions of the concerns between younger and older players. Furthermore, gender matters for two of the four dimensions." Try to go more in-depth and to develop explanations!

Reply: We elaborated in more detail on the differences between younger and older players and male and female players. We showed that these results are in line with findings from previous literature. (#5)

Reviewer 1 Comment 6: Chair? There are two co-authors (Harborth + Pape). Are BOTH the "Chair" of the faculty/department mentioned on p1?

Reply: Chair refers to the research group (an organizational unit below department). We are both not holding the chair.

Reviewer 1 Comment 7: Abbreviations: Several abbreviations would be worthwhile avoiding. Pokmon Go is always worthwhile spelling out in full.

Reply: We spelled it out in full.

Reviewer 1 Comment 8: Editing: The paper may benefit from a final read-through by an Anglophone editor/proof-reader (e.g., section 3.3. "educational degrees" is incorrect = either educational "qualifications" or educational "certificates").

Reply: Unfortunately, we do not have access to a native speaker. But we tried to improve and asked several colleagues to proof-read.

Reviewer 1 Comment 9: Length: Last but not least, at 17 pages - with 59 references, the paper seems to exceed the recommended page-length for the summer school publication. It should be shortened.

Reply: The paper is now 16 pages.

Reviewer 2 Comment 1: The privacy discussion in Section 2.2 seems a bit superficial and far too broad. Yes, it is interesting how different definitions of privacy look like. But wouldn't it be better to be a bit more specific about privacy risks associated to using augmented reality and location based services in particular? From my point of view the paper would benefit from this. The discussion on the privacy paradox in Section 2.2 though is nice.

Reply: We shortened this paragraph according to your suggestions, especially the privacy definitions. Potential privacy risks are already discussed in the Introduction, whereas the literature on this topic is relatively sparse [22].

Reviewer 2 Comment 2: I am still not quite sure if the questionnaire is really specific enough for the setting of location-based augmented reality games such as Pokemon Go, as most of the question could be used for an arbitrary use of the smartphone or playing arbitrary games on smartphones.

Reply: The questionnaire follows well established constructs from information systems research. Unfortunately, in particular for AR, there are no more specific constructs. Thus, we had to decide whether we want to design our own constructs and risk that they are not validated, thus participants understand questions in a different way than we had in mind or go with validated, well-established constructs which may be not specific, but are suitable for the context. It was one of the first surveys, thus we do think that the result is of interest and worth to publish. Although, further work here is welcomed.

Reviewer 2 Comment 3: It should be made clear what [25] does. Ideally in the introduction of the paper it should be stated that "In [25] the authors already discuss ... but do not focus on privacy aspects" (at least from what I understand when looking at the abstract of [25]).

Reply: [25] is [23] now. This paper builds upon the same data set, but describes the demographics in a greater detail, including plots of the distribution of the single demographics. Therefore, we referred to the paper for additional information.

Reviewer 2 Comment 4: It may have also been interesting to aks the people whether they consider themselves as being "tech-savvy".

Reply: We had this in mind, but had to restrict our self in the number of questions to not exaggerate with the length of the questionnaire. Besides the questions shown here, we had several others where we are still working on the evaluation. For the future we have in mind to apply the The Online Privacy Literacy Scale (OPLIS).

Reviewer 3 Comment 1: The authors forgot to put keywords, and email addresses which are also missing.

Reply: Thanks for mentioning this. We have fixed it.

Reviewer 4 Comment 1: The study is based only in Germany (reasons explained). Comparing the results with other geographical location might have improved the insights of the results

Reply: Thanks for mentioning this. As discussed in the Limitations and Future Work sections, this was not part of this study but provides the foundation for further work.

Reviewer 4 Comment 2: Any Implication/suggestion suggestion for privacy related games based on the results (age, gender) could have improved the value of contribution

Reply: Since we are only investigating one game in this paper and neither providing a survey not introducing an own approach for a game, we couldn't address this issue within the given page count.

Reviewer 5 Comment 1: There are some typographical errors that should be corrected as given below:

Reply: Thank you (and all other reviewers). We proof-checked the paper and hopefully eliminated all typographical errors.