Northumbria Research Link

Northumbria
University
NEWCASTLE

A Two-Pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality Applications

David Harborth
Goethe University Frankfurt, Germany
david.harborth@m-chair.de

Majid Hatamian
Goethe University Frankfurt, Germany
majid.hatamian@m-chair.de

Welderufael B. Tesfay
Goethe University Frankfurt, Germany
Welderufael.Tesfay@m-chair.de

Kai Rannenberg
Goethe University Frankfurt, Germany
kai.rannenberg@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 currently focusing primarily on mobile AR (MAR) technologies, i.e. applications on mobile devices, like smartphones or tablets. Associated privacy issues have to be investigated early to foster market adoption. This is especially relevant since past research found several threats associated with the use of smartphone applications. Thus, we investigate two of the main privacy risks for MAR application users based on a sample of 19 of the most downloaded MAR applications for Android. First, we assess threats arising from bad privacy policies based on a machine-learning approach. Second, we investigate which smartphone data resources are accessed by the MAR applications. Third, we combine both approaches to evaluate whether privacy policies cover certain data accesses or not. We provide theoretical and practical implications and recommendations based on our results.

1. Introduction

The release of Pokémon Go in 2016 led to a major boost in public awareness about augmented reality (AR) [1, 2]. AR 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" [3, p. 34]. The increasing awareness also led to discussions on privacy issues related to the use of Pokémon Go [4]. After Apple (ARKit) and Google (ARCore) released the AR development kits in 2017, the AR features started to become better [5] and many new mobile AR (MAR) applications (apps) diffused into the consumer market since then. Nowadays, the majority of people experience AR mainly by interacting with MAR apps on their regular mobile devices since AR glasses like the Microsoft Hololens [6] are not mature enough and too expensive for the mass market. Thus, MAR apps shape the perceptions of millions of users about AR. These perceptions can also be influenced by privacy concerns and threats [7]. Thus, it is necessary to investigate privacy issues for new technologies when they diffuse into the market. However, AR is not widely investigated in the information systems (IS) domain [8]. Previous studies on MAR applications show that privacy concerns are prevalent among the users [9]. In addition, past analyses on smartphone application behaviors show accesses on a diversity of personal information stored in the mobile devices [10, 11]. Furthermore, literature indicates that privacy policies of apps are difficult to understand by regular users [12] which can lead to a loss of trust and a decreasing probability of acceptance [13]. However, to the best of our knowledge, there is no research which combines these aspects and investigates potential privacy issues arising from the privacy policies and the resource access behaviors of MAR apps. Thus, we address the following research questions:

1. *Are the data processing practices stated in the privacy policies of the selected MAR applications beneficial for the user's privacy?*
2. *What resources of the mobile device are accessed by the MAR applications and are these accesses privacy-invasive or relevant to the proper functionality of such applications?*
3. *Do the selected MAR applications access resources according to the theoretical behavior stated in the associated privacy policies?*

We base our analysis on 19 of the most prominent MAR applications (with respect to downloads) from

This research was partly funded by the German Federal Ministry of Education and Research (BMBF) with grant number: 16KIS0371 and has received funding from the H2020 Marie Skłodowska-Curie EU project "Privacy&Us" under the grant agreement No 675730.

URI: https://hdl.handle.net/10125/59940
ISBN: 978-0-9981331-2-6

the Google Play Store. We analyze the privacy policies with a machine-learning based tool according to eleven aspects of the European General Data Protection Regulation (GPDR). The resource accesses of the MAR apps are assessed by installing a monitoring app on an Android smartphone. In a final step, we synthesize the results by comparing the resource accesses with the statements of the privacy policies.

The remainder of the paper is structured as follows. Related work is presented in Section 2. The methodology is described in Section 3 and the results are presented in Section 4. We conclude by discussing the results and implications of our work in Section 5.

2. Related Work

The related work section is structured in three parts. First, we present the related work on the intersection of AR, especially MAR, and privacy. Since we use two different methods to assess possible privacy issues of MAR applications, we summarize current research on privacy policies and the investigated privacy issues as well as related research on the analysis of the privacy behavior of smartphone apps.

2.1. Privacy in (mobile) augmented reality

Since AR and privacy are investigated in different disciplines, we searched for articles about privacy issues in MAR in the IS domain, in the specific domain dealing with mixed and augmented reality and in the human-computer interaction (HCI) domain.

Research on privacy is a widely investigated topic in the IS domain [14]. However, privacy topics associated with AR technologies are not investigated in the IS domain up to now [8]. There are several articles on technology acceptance of AR technologies (e.g. [15, 16]) and brief essays on possible privacy issues related to AR (e.g. [17, 18]). However, to the best of our knowledge, there is no empirical research in the IS domain aiming at the intersection of AR and privacy.

Dey et al. [19, 20] conduct a literature review on past user studies on AR. Their results show an increase in user-focused studies (e.g. [21, 22]). However, to the best of our knowledge, there are also no specific articles dealing with privacy issues of AR technologies.

The search in the HCI discipline shows that there is research which considers privacy aspects. For example, Koelle et al. [23] find, that the use of data glasses can be perceived as privacy-invasive. This especially holds for possible bystanders around the user of the AR technology. Similar results are found by Denning et al. [24], whereas the authors only focus on bystanders around AR devices. Both studies investigate data glasses as a type of AR technology. In summary, it can be seen that there is a gap with respect to privacy and AR technologies. This is especially true for MAR technologies since these are less investigated in the literature. The practical importance of privacy research on MAR apps is given due to the relatively large diffusion into the mass market compared to other AR technology types. This is underpinned by the current efforts of large technology companies like Apple or Google to establish the best AR features in their operating systems and associated mobile devices [5].

2.2. Privacy Policy Analyses

Costante et al. [25] proposed a method for evaluating the completeness of privacy policies, using Natural Language Processing (NLP) and Machine Learning (ML) techniques, where a privacy policy is said to be *complete* if it contains descriptions which should be explained in privacy policies, such as how to deal with cookies. Similarly, Guntamukkala et al. [26] proposed a method for evaluating the completeness of privacy policies mainly following a new evaluation criteria called goal-based approach. Terms of Service: Didn't Read (ToS:DR) is a community based project which valuates privacy policies by crowd-sourcing, and also provides an add-on for a browser [27]. Zimmeck et al. [28] use results of ToS:DR to derive privacy aspects and develop Privee, a machine learning and NLP based tool. Kelley et al. [29] and Gluck et al. [30] show that the use of condensed and standardized privacy notices has a positive effect on user's awareness of privacy practices.

2.3. Smartphone application behavior analysis

Agarwal et al. [31] introduce the *ProtectMyPrivacy* system for iOS which exposes accesses to sensitive resources by mobile apps. Based on this, users can decide to anonymize private information and share these decisions with others. Thus, a crowdsourced recommendation engine is designed to recommend privacy settings to the users. Enck et al. [32] investigate the privacy of smartphone apps in a different way. Instead of looking at single permissions individually, they suggest to monitor a set of sensitive permissions, e.g. location, gallery, contacts, phone number, etc. In a sample of 311 of the most popular apps downloaded from Google Play, they find five apps that implement dangerous functionalities and therefore should be installed with extreme caution. Followed by this study, Enck et al. [33] aim to better understand the security in smartphone apps by proposing a decompiler which recovers Android apps source code directly from its installation image. They analyze 21 million lines of

recovered code from 1,100 free apps using automated tests and manual inspection and it shows the use/misuse of personal/phone identifiers, and deep penetration of advertising and analytics networks.

TaintDroid [34] is a method in which the behavior of 30 popular Android apps is studied. The analyses shows that two-third of the apps show suspicious handling of sensitive data and that 15 of them reported users' location to remote advertising servers. *Styx* [35] is the name of a conceptual model which is based on TaintDroid. Styx is aimed to efficiently communicate the privacy impacts of smartphone apps to its users. Results of a user study indicate that Styx is able to increase user trust into smartphone platforms and also reduce privacy concerns through communicating efficient privacy warnings. Similar to our approach, Kununka et al. [36] compare actual data practices with the privacy policies. They find that there is a potential personal data disclosure to third-parties by app providers which is not stated in the respective privacy policy. However, in contrast to our study, they analyze a relatively small set of the potential data on the smartphone which is disclosed to third parties. The information on the data disclosure to third-parties is taken from another paper by Zang et al. [37] who follow a man-in-the-middle approach to gather the connections between apps and external servers. In contrast, by installing the monitoring tool and the smartphone itself (cf. Section 3.3) we are able to gather more granular information of resource accesses (cf. Table 2).

3. Methodology

The methodology is based on two pillars which rest on already developed and tested tools to analyze privacy policies [38, 39] and app resource access behaviors [**?**]. The contribution of this paper is the synthesis of both approaches and the app to MAR apps. Thus, the methodology has three concrete steps of analyses (cf. Figure 1). First, we analyze the privacy policies for every app in our sample based on a machine-learning approach (Sections 3.2). Since policies only provide a theoretical statement on what apps and the providers do with the user data, we analyze the actual MAR app behavior in a second step (Section 3.3). Finally, we synthesize the results by comparing the app behavior with the statements in the respective privacy policies.

3.1. MAR application selection

We analyzed a total of 19 MAR apps (see Table 3 for the details of app names and IDs). We focus on Android MAR apps running only with ARCore from the German Google Play Store. We implemented

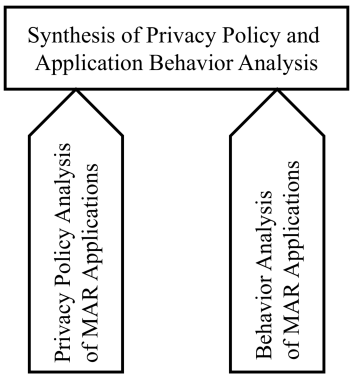

Figure 1. Overview of the methodology

the privacy behavior analysis tool for Android devices because of two reasons. First, Android dominates the market share with a share of 85.1% (2017) and the number of available Android apps on the Google Play Store recently was placed at 3.8 million apps [40, 41]. Second, according to recent observations, Android is the most vulnerable operating system in the world with 841 vulnerabilities that enable unauthorized parties to gain access to the sensitive device resources [42]. Accordingly, we were interested to mainly focus on this operating system. The apps were selected based on a current study on the most downloaded MAR apps in the Apple App Store [43]. We had to transfer the results from this study since there is, to the best of our knowledge, no comparable estimation available for Android at the moment. Since we did not want to only focus on free apps, we also included six apps with a single payment pricing scheme. Most of the selected apps (eleven out of 19) are games.

3.2. Privacy policy analysis of MAR applications

Privacy policies serve as the binding contractual agreements between users and service providers [44], i.e., MAR app service providers in our specific scenario. Privacy policies are also the defacto transparency boards where MAR app service providers communicate their data processing practices to their users. However, numerous studies show that users rarely read these documents owing to their natural technicality and excessive length that makes them difficult to be comprehended by ordinary users [12, 45, 46]. To address this pertinent challenge, we proposed an automatic machine learning based tool, PrivacyGuide, in our previous works [38, 39]. The objective of PrivacyGuide is to summarize lengthy privacy policy documents and present them in condensed and

easy to understand notes. We refer the reader to these two papers for in depth insights about the the tool. PrivacyGuide considers eleven aspects for the privacy policy analysis which are defined taking the European Union (EU) General Data Protection Regulation (GDPR) into account. These aspects include data collection, security, control, aggregation, deletion, retention, breach notification, protection of children data, third party sharing, privacy policy changes, and settings. However, despite the fact that the GPDR now clearly mentions the privacy breach notification as responsibility for the service provider, none of the privacy policy we analyzed have any mention about notification plans. In order to draw the attention of users, PrivacyGuide takes a risk based approach to the analysis of the privacy policy documents. It considers a three scale risk analysis where green represents good data processing practices (explicit statements on the collected data types or a collection of a small set of data types), while red shows the opposite (either no information about what is being collected or a collection of a large amount of data), and yellow indicates a scale in between these two. The privacy policies were analyzed before and after the official application date of the GDPR on May 25, 2018. By that, we wanted to assess to what extent the app providers changed their policies for European users. Eight app providers changed their policy for the GDPR. The results for the machine-learning policy analysis improved from a privacy point of view. Due to space limitations, we will only report the detailed results for every MAR app for the time after May 25, 2018 since these are the ones that should still be valid for future comparisons of this work.

3.3. Privacy behavior analysis of MAR applications

In order to analyze the privacy behavior of MAR apps, we used a tool called Android Apps Behavior Analyzer (A3), which was developed and tested in an earlier work of the authors [47, 48]. A3 is solely designed and implemented for Android devices. Technically it benefits from two main components, namely log reader and data mining components. The log reader component is responsible to read the logs produced by the users device. This includes all the resource accesses by the installed apps (e.g. access to sensitive resources like `CAMERA`, `READ_CONTACTS`, `LOCATION`, etc.). Additionally, the app records timestamps and the total number of resource accesses. The data produced by this component is processed and fed into the data mining component. This component is a rule-based engine that comprises several rules to identify potential privacy invasive activities by the users installed apps. We installed the A3 tool on a Samsung Galaxy S8+ with the OS Android 7.0. At the time of our experiment, ARCore version 1.2 was not yet published. Thus, the results only hold for the previous version.

To analyze the privacy behavior of our selected MAR apps, we conducted the experiment in two phases, while the A3 tool was running in the background the whole time (i.e. it was monitoring the privacy behavior of MAR apps). In the first phase (ranging from May 14 to May 18), we interacted actively with the mobile device and used the MAR apps on a daily basis. We ran the MAR apps once and let them to be executed in the background during the second phase (ranging from May 18 to May 21). Thus, we never interacted with the mobile device during this time.

4. Results

In this section, we present the results for the privacy policy and privacy behaviour analysis as well as the synthesis of both analyses.

4.1. Results of the privacy policy analysis

The outcomes of the risk-based analysis are shown in Table 4. We analyze the outcomes for each app and aspect and build the sums over the different aspects per app as well as over the different apps per aspect.

The privacy policies of the selected MAR apps indicate that the app providers have bad data processing practices (100 out of 190 outcomes are red). This is especially true for the information about protection of children, third-party sharing, data retention, control of data, privacy settings and account deletion. Furthermore, there are eight apps with more than 5 outcomes that are analyzed as red.

4.2. Results of the privacy behavior analysis

In total, seven sensitive resources were accessed by the MAR apps (Table 1)[1]. The results of the analysis for every app and resource are shown in Table 2. Each cell contains the results for the active and passive phase.

There is a significant decrease in the number of resources accesses from the active phase 1 to the passive phase 2. In general, we would assume that the resource accesses decrease to zero during the passive phase since there is no interaction with the apps and the smartphone itself. However, this is not the case in our study. Thus, we marked every privacy deviated behavior or privacy misbehavior of the app in bold face if the app:

[1] https://developer.android.com/guide/topics/permissions/overview

Table 1. Identified permissions accessed by examined MAR apps.

Permission	Description
READ_STORAGE	*Allows an app to read from external storage.*
CAMERA	*Required to be able to access the camera device.*
BODY_SENSOR	*Allows an app to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.*
READ_CONTACTS	*Allows an app to read the user's contacts data.*
LOCATION	*Allows an app to access location.*
PHONE_STATE	*Allows an app to access the phone state, including phone number of the device, current cellular network information, the status of any ongoing calls, the list of any phone accounts registered on the device and a verification of the user/phone with IMEI information*
RECORD_AUDIO	*Allows an app to record audio.*

- accessed resources besides the storage during the passive phase, or
- accessed resources in the active phase which are not required for the app use.

We define a required resource for the app use as an obvious and ease to understand need of the app to function properly. For example, a location-based app necessarily needs access to the location. Another example in our sample is app 9 (Insight Heart) and one access to the body sensor. Since this MAR app has the feature of synchronizing the user's own heartbeat with the digital heart, we assume that this app accessed the body sensor once during the first start of the app.

According to the definition of privacy misbehavior, we discuss the results in bold face for every resource type. The storage accesses are not surprising during the two phases since the phone was not completely turned off. However, three apps accessed the camera twice in the passive phase (app 4, 6 and 14). These accesses are privacy-invasive, since the user does not know that the app currently accesses the camera. Contacts were accessed by app 13 during the active phase. In general, such accesses to the contacts should not be done by apps. In this case the app is a game (Monster Park AR), where it is not clear why it needs access to the user's contacts. Thus it is important to assess the privacy policy of the app to assess to what extent this information is needed. As discussed earlier, accesses to the location must not be a problem for the user's privacy in general. However, app 11 accesses the location 21 times in the active phase and 4 times in the passive phase. This is problematic from a privacy point of view in both phases since the app is not a location-based and, therefore, does not need the location information to function.

The phone state is an interesting data resource since the respective information is highly privacy sensitive. This permission enables an invasive party to gain access to sensitive resources such as phone number, cellular network information, outgoing call information, etc. Most of the accesses to this resource happened mainly during the active phase (except for app 1 which also accessed this resource twice in the passive phase). The only relevant reason to access this permission is to stop the app when there is an ongoing call, however, we did not use any SIM card on the device, therefore, there is no obvious reason of such resource access. Thus, several MAR apps behave not privacy-friendly in this resource category. The last resource which was accessed by two apps is the recording of audio data. We did not see any feature needing access to the microphone when we interacted with both apps. Thus, these accesses can be seen as not privacy-friendly.

In summary, eleven apps misbehaved with respect to the user's privacy (gray rows). In a next step, we assess whether the accesses marked as not privacy-friendly in this section are stated in the associated privacy policies.

4.3. Synthesis of the analyses

The privacy policy of the first app states that the phone number *may* be collected. This corresponds to the identified accesses of the phone state. However, there is no information provided on why this data is needed other than *"Personal information identifies you and may be used to contact you online or offline"*. Since an access to the phone state makes it possible to collect all the information defined in Table 1, it is necessary to specifically state which types of information are gathered and how they are used. This result is in line with the machine-learning based policy analysis in Table 4. The data collection practices are yellow, indicating that the policy contains ambiguous or unclear statements about the collected data. The same holds for the second app, whereas there were less accesses to the phone state in the active phase and no access in the passive phase. The privacy policy is also mentioning the phone number as a type of collected data.

The behavior of app 6 accessing the camera twice in

Table 2. MAR application behaviors (active phase versus inactive phase)

	Resource Accesses Phase 1 – Phase 2						
App #	READ_ STORAGE	CAMERA	BODY_ SENSOR	READ_ CONTACTS	LOCATION	PHONE_ STATE	RECORD_ AUDIO
1	17 – 2	18 – 0	0 – 0	0 – 0	0 – 0	**12 – 2**	0 – 0
2	18 – 6	10 – 0	0 – 0	0 – 0	0 – 0	**2 – 0**	0 – 0
3	14 – 4	10 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
4	10 – 1	**10 – 2**	0 – 0	0 – 0	0 – 0	**3 – 0**	0 – 0
5	17 – 2	14 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
6	10 – 11	**11 – 2**	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
7	12 – 8	14 – 0	0 – 0	0 – 0	0 – 0	**3 – 0**	0 – 0
8	11 – 4	8 – 0	0 – 0	0 – 0	0 – 0	**9 – 0**	0 – 0
9	7 – 11	10 – 0	1 – 0	0 – 0	0 – 0	0 – 0	0 – 0
10	10 – 3	8 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
11	19 – 11	12 – 0	0 – 0	0 – 0	**21 – 4**	0 – 0	0 – 0
12	8 – 10	10 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
13	13 – 9	14 – 0	0 – 0	**3 – 0**	0 – 0	0 – 0	**4 – 0**
14	8 – 5	**6 – 2**	0 – 0	0 – 0	0 – 0	**2 – 0**	0 – 0
15	15 – 3	10 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
16	7 – 7	10 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
17	9 – 3	10 – 0	0 – 0	0 – 0	0 – 0	0 – 0	0 – 0
18	11 – 8	12 – 0	0 – 0	0 – 0	0 – 0	0 – 0	**1 – 0**
19	14 – 6	10 – 0	0 – 0	0 – 0	0 – 0	**9 – 0**	0 – 0

the passive phase is not mentioned in the privacy policy. The same holds app for 4 accessing the camera twice in the passive phase. The privacy policy does not state anything on potential camera accesses when the app is not used. In addition, phone state data were collected and it is stated in the policy that they may collect data like *device identifiers [or] IP address*. However, there is no explicit information what data is exactly collected and for what purpose. The PrivacyGuide analyzes the policy as green with respect to data collection practices. This might be due to the false positive generalization. Accesses to the phone state were also exerted by apps 7, 8 and 19 during the active phase. The privacy policy of app 7 explicitly states the need to access the phone state for *ad services or Inapp services* whereas it is unclear which specific types of information are processed. The policy of app 19 is more specific with respect to phone state associated information by stating to collect, among others, *identifiers such as IP address, device identifiers [or] ad identifiers*. As for previous apps, it is also not listed which specific data types are processed. In contrast to apps 7 and 19, app 8 does not state anything about collecting phone state related data.

App 11 accessed the location data several times during the active phase and even during the passive phase. The privacy policy states a possible collection of *broad geographic location (e.g. country or city-level location)* data. However, this is only stated for the case of *When you visit our Sites [i.e. the MAR app], we may collect certain information automatically from your device*. Thus, the accesses to the location in the passive phase are not explained by the privacy policy.

Both, accesses to the contacts as well as the audio resources are not described in the privacy policy of app 13. The same holds for the accessed audio resource by app 18. The privacy policy does not mention the use of audio data at all. A special case is app 14 (Porsche Mission E). Here, the link to the privacy policy in the Google Play Store only leads to a legal notice. This is quite puzzling since there should be a policy available for the users of this app. The necessity for a privacy policy is underpinned by the privacy-invasive accesses to the camera in the passive phase and the phone state. When comparing the results of the machine-learning based privacy policy analysis for app 14 with the fact that there is no policy, it becomes obvious that the tool produced a false positive for the aspect data aggregation (the accuracy for the risk analysis is 90% [39]).

5. Discussion and Conclusion

Our results indicate that there is a privacy risk associated with the majority of the most famous Android MAR apps. This risk arises due to bad data processing practices stated in the privacy policies and privacy misbehaviors of the applications. Our results show

several accesses to highly sensitive information like the contacts, the microphone, the location or the phone state. In addition, several resources were accessed during the passive phase, in which the smartphone was not used actively. None of the resource accesses in the passive state are explained by the privacy policies. Several accesses in the active phase (e.g. of contacts or audio) are also not explained. Thus, the user is exposed to undisclosed privacy risks. This is important to notice when discussing user behavior with respect to privacy and as well as the necessity of regulations (e.g. the GDPR). Against this backdrop, models on privacy related behavior of users are problematic and regulations become necessary when users do not have the chance to get correct and full information about data collection and disclosure of applications (shown by the gap between app behaviors and privacy policies).

Thus, we argue that MAR developers should carefully investigate the required permissions by their apps. Our study confirmed that over-privileged MAR apps (apps with unnecessary and aggressive access to sensitive resources) are an issue which needs to be addressed. We also highlight that MAR app privacy policies need to be severely revisited by their developers. We also recommend the MAR developers to revise their privacy policies with respect to unrelated content. We observed that there is a significant number of privacy policies that do not focus on the application itself, but the developer's webpage, the services offered/provided by the developers and other unrelated content to the app's privacy practices. These steps are necessary to protect the user's right for privacy during the use of MAR apps. In addition, this is necessary for a wider acceptance of this relatively new technology. Previous studies show that privacy concerns can have a direct or indirect negative impact on the adoption and use of new technologies and services [49, 7].

At the time of our study, the number of available Android MAR apps was rather small, especially since we aimed to consider apps with high download numbers. Since we expect a continuing increase in available MAR apps, future work should consider to increase the sample size and investigate more MAR applications. Our work contributes to the literature by filling the gap between MAR and privacy. Furthermore, studies like ours can help to improve the users privacy by creating awareness and an advanced understanding about privacy threats.

References

[1] J. Nicas and C. 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.

[2] R. Kh, "Augmented Reality Gets Boost From Pokemon Go." https://www.engadget.com/2016/09/28/augmented-reality-gets-boost-from-pokemon-go/, 2016.

[3] R. T. Azuma, Y. Baillot, S. Feiner, S. Julier, R. Behringer, and B. Macintyre, "Recent Advances in Augmented Reality," in *IEEE Computer Graphics And Applications*, no. November/December, pp. 34–47, 2001.

[4] A. Peterson, "Pokémon Go had 'full access' to the Google accounts of some iPhone players." https://www.washingtonpost.com/news/the-switch/wp/2016/07/12/pokemon-go-had-full-access-to-the-google-accounts-of-some-iphone-players/, 2016.

[5] S. Nellis, "Google, Apple face off over augmented reality technology." https://www.reuters.com/article/us-google-apple/google-apple-face-off-over-augmented-reality-technology-idUSKCN1BA001, 2017.

[6] Microsoft, "Microsoft HoloLens." https://www.microsoft.com/microsoft-hololens/en-us/buy, 2017.

[7] C. M. Angst and R. Agarwal, "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MISQ*, vol. 33, no. 2, pp. 339–370, 2009.

[8] D. Harborth, "Augmented Reality in Information Systems Research: A Systematic Literature Review," in *Twenty-third Americas Conference on Information Systems (AMCIS)*, (Boston), pp. 1–10, 2017.

[9] D. Harborth and S. Pape, "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.), pp. 314–329, Springer, Cham, 2018.

[10] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *CHI '13*, pp. 3393–3402, 2013.

[11] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: installing applications on an android smartphone," in *26th FC'*, pp. 68–79, 2012.

[12] A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, "Availability and quality of mobile health app privacy policies," *Journal of the American Medical Informatics Association*, vol. 22, no. e1, pp. e28–e33, 2014.

[13] G. Bansal, F. M. Zahedi, and D. Gefen, "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern," *European Journal of Information Systems*, vol. 24, pp. 624–644, 2015.

[14] H. J. Smith, T. Dinev, and H. Xu, "Theory and Review Information Privacy Research: An Interdisciplinary Review," *MISQ*, vol. 35, no. 4, pp. 989–1015, 2011.

[15] A. Salinas Segura and F. Thiesse, "Extending Utaut2 To Explore Pervasive Information Systems," *ECIS 2015 Proceedings*, pp. 1–17, 2015.

[16] H. F. Ross and T. Harrison, "Augmented Reality Apparel: an Appraisal of Consumer Knowledge, Attitude and Behavioral Intentions," in *HICCS Proceedings 2016*, pp. 3919–3927, 2016.

[17] J. Hong, "Considering privacy issues in the context of Google glass," *Communications of the ACM*, vol. 56, no. 11, pp. 10–11, 2013.

[18] F. Roesner, K. Tadayoshi, and D. Molnar, "Security and Privacy for Augmented Reality Systems," *CACM*, vol. 57, no. 4, pp. pp. 88–96, 2014.

[19] A. Dey, M. Billinghurst, R. W. Lindeman, J. E. S. II, and J. E. Swan II, "A Systematic Review of Usability Studies in Augmented Reality between 2005 and 2014," in *2016 IEEE International Symposium on Mixed and Augmented Reality, ISMAR Adjunct*, pp. 49–50, 2016.

[20] A. Dey, M. Billinghurst, R. W. Lindeman, and J. E. Swan, "A Systematic Review of 10 Years of Augmented Reality Usability Studies: 2005 to 2014," *Frontiers in Robotics and AI*, vol. 5, no. April, pp. 1–28, 2018.

[21] T. Olsson and M. Salo, "Online User Survey on Current Mobile Augmented Reality Applications," in *ISMAR*, pp. 75–84, 2011.

[22] D. Harborth and S. Pape, "Exploring the Hype: Investigating Technology Acceptance Factors of Pokémon Go," in *International Symposium on Mixed and Augmented Reality (ISMAR)*, pp. 155–168, 2017.

[23] M. Koelle, M. Kranz, and A. Möller, "Don't look at me that way! Understanding User Attitudes Towards Data Glasses Usage," in *MobileHCI '15*, pp. 362–372, 2015.

[24] T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses," in *CHI '14*, pp. 2377–2386, 2014.

[25] E. Costante, Y. Sun, M. Petković, and J. den Hartog, "A machine learning solution to assess privacy policy completeness," in *ACM WPES*, pp. 91–96, 2012.

[26] N. Guntamukkala, R. Dara, and G. Grewal, "A machine-learning based approach for measuring the completeness of online privacy policies," in *14th International Conference on Machine Learning and Applications (ICMLA)*, pp. 289–294, IEEE, 2015.

[27] ToS:DR, "Terms of service: Didn't read (tos:dr)." `https://tosdr.org/index.html`, 2018.

[28] S. Zimmeck and S. M. Bellovin, "Privee: An architecture for automatically analyzing web privacy policies.," in *USENIX Security Symposium*, pp. 1–16, 2014.

[29] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing privacy notices: an online study of the nutrition label approach," in *CHI '10*, pp. 1573–1582, 2010.

[30] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal, "How short is too short? implications of length and framing on the effectiveness of privacy notices," in *SOUPS 2016*, 2016.

[31] Y. Agarwal and M. Hall, "Protectmyprivacy: detecting and mitigating privacy leaks on ios devices using crowdsourcing," in *MobiSys*, pp. 97–110, 2013.

[32] W. Enck, M. Ongtang, and P. Mcdaniel, "On lightweight mobile phone application certification," in *16th ACM CCS*, pp. 235–245, 2009.

[33] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in *20th USENIX Conference on Security*, pp. 21–21, 2011.

[34] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," in *9th ACM USENIX Conference on Operating Systems Design and Implementation*, pp. 393–407, 2010.

[35] G. Bal, K. Rannenberg, and J. Hong, "Styx: Privacy risk communication for the android smartphone platform based on apps' data-access behavior patterns," *Computers & Security*, vol. 53, pp. 187–202, 2015.

[36] S. Kununka, N. Mehandjiev, and P. Sampaio, "A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices versus Compliance to Privacy Policy," 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.), pp. 303–313, Springer, 2018.

[37] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps," *Technology Science*, 2015.

[38] W. B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, "I read but don't agree: Privacy policy benchmarking using machine learning and the eu gdpr," in *The WWW Conf. 2018*, pp. 163–166, 2018.

[39] W. B. Tesfay, P. Hofmann, T. Nakamura, S. Kiyomoto, and J. Serna, "Privacyguide: Towards an implementation of the eu gdpr on internet privacy policy evaluation," in *4th ACM IWSPA*, pp. 15–21, 2018.

[40] Statista, "Market share worldwide smartphone shipments by operating system from 2014 to 2022." `https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/`, 2017.

[41] Statista, "Number of apps available in leading app stores as of 1st quarter 2018." `https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/`, 2018.

[42] Cybrnow, "10 most vulnerable os of the year 2017." `http://www.cybrnow.com/10-most-vulnerable-os-of-2017/`, 2018.

[43] SensorTower, "Arkit-only apps surpass 13 million downloads in first six months, nearly half from games." `https://sensortower.com/blog/arkit-six-months`, 2018.

[44] S. Wilson, F. Schaub, A. A. Dara, F. Liu, S. Cherivirala, P. G. Leon, M. S. Andersen, S. Zimmeck, K. M. Sathyendra, *et al.*, "The creation and analysis of a website privacy policy corpus.," in *ACL (1)*, 2016.

[45] R. W. Proctor, M. A. Ali, and K.-P. L. Vu, "Examining usability of web privacy policies," *Intl. Journal of Human–Computer Interaction*, vol. 24, no. 3, pp. 307–328, 2008.

[46] R. A. Cadogan, "An imbalance of power: the readability of internet privacy policies," *Journal of Business & Economics Research (JBER)*, vol. 2, no. 3, 2011.

[47] M. Hatamian and J. Serna-Olvera, "Beacon alarming: Informed decision-making supporter and privacy risk analyser in smartphone applications," in *2017 IEEE ICCE*, pp. 468–471, 2017.

[48] M. Hatamian, J. Serna, K. Rannenberg, and B. Igler, "FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps," in *Trustbus 2017*, pp. 1–16, 2017.

[49] C. V. Slyke, R. Johnson, J. Jiang, and J. Shim, "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems*, vol. 7, no. 6, pp. 415–444, 2006.

All websites were last accessed on June 14, 2018.

A. MAR application information and privacy policy analysis results

Table 3. Google Play Store ID, Privacy Policy URL and Pricing Scheme of the MAR Applications

MAR Application Name	Google Play Store Link	Privacy Policy URL	Pricing
1) AMON	id=com.lykkestudios.amon	https://www.lykkestudios.com/privacy/	€2.99
2) ARise	id=com.ClimaxStudios.Aris	http://www.climaxstudios.com/privacy-policy/	€3.29
3) Army of Robots	id=com.sinergiastudios.armyofrobots	http://sinergiastudios.com/EULA/ ArmyOfRobots/terms-en.html	free
4) CamToPlan	id=com.tasmanic.camtoplan	http://misc.tasmanic.com/camtoplanpolicy.html	€3.99
5) Capsule Commander AR	id=com.Duncan.CCAR	https://sites.google.com/view/ccprivacypol/home	free
6) Doll House Decoration - AR	id=com.unitm.android.dollhousedecorationar	http://unitmgames.com/Privacy-Policy.html	
7) Froggie Jump	id=com.CendaGames.FroggieJumpFree	http://cenda.cz/privacy.html	free
8) IKEA Place	id=com.inter_ikea.place	http://www.ikea-place.com/privacy-policy/	free
9) Insight Heart	id=com.animares.heart	https://animares.com/privacy-policy	€2.29
10) Jenga AR	id=com.freerangegames.jengaar	http://freerangegames.com/privacypolicy/	free
11) Knightfall AR	id=com.aetn.games.android.history.knightfall.ar	http://www.aenetworks.com/privacy	free
12) Mind Map AR, Augmented Reality ARCore Mind Mapping	id=com.scapehop.mindmapar	https://www.iubenda.com/privacy-policy/8170925	free
13) Monster Park AR - Dinosaurier AR: Jurassic Welt	id=com.vitotechnology.DinoAR	http://vitotechnology.com/privacy-policy.html	free
14) Porsche Mission E	id=com.porsche.missionear	https://www.porsche.com/international/legal-notice/	free
15) Slingshot Island	id=com.socketheadgames.slingshotisland	http://www.socketheadgames.com/Privacy-Policy	€0.99
16) Solar System AR (ARCore)	id=com.guidapasquale.solarsystemar	https://guidapasquale.wordpress.com/privacy-info/	free
17) The Machines	id=com.directivegames.themachines.android	http://directivegames.com/privacypolicy.html	€4.69
18) World of Tanks AR Experience	id=net.wargaming.wot.ar	http://legal.eu.wargaming.net/de/ datenschutz-und-cookie-richtlinie/	free
19) Zombie Gunship Revenant AR	id=com.limbic.revenant	https://www.limbic.com/privacypolicy/	free

Table 4. Privacy Policy Analysis Results (after May 25, 2018)

	Privacy Aspects of the General Data Protection Regulation (GDPR)										**Sums**		
App #	Data Collection	Protection of children	Third-Party sharing	Data security	Data retention	Data aggregation	Control of Data	Privacy settings	Account deletion	Policy changes	$\sum_G$	$\sum_Y$	$\sum_R$
1	yellow	green	red	green	green	yellow	green	red	red	yellow	4	3	3
2	yellow	red	red	green	red	yellow	yellow	red	red	green	2	3	5
3	green	green	red	green	yellow	yellow	red	red	green	green	5	2	3
4	green	red	red	red	red	yellow	red	yellow	red	yellow	1	3	6
5	red	red	red	red	red	green	red	red	red	red	1	0	9
6	red	green	red	red	red	green	red	red	red	red	2	0	8
7	red	red	red	red	red	yellow	red	red	red	red	0	1	9
8	yellow	red	yellow	green	yellow	green	green	red	red	red	3	3	4
9	red	red	red	red	red	green	red	red	red	green	2	0	8
10	green	green	red	green	red	yellow	green	green	green	yellow	6	2	2
11	yellow	green	red	green	yellow	red	green	green	green	green	6	2	2
12	green	red	red	green	yellow	green	red	red	green	yellow	4	2	4
13	yellow	green	red	green	red	yellow	red	yellow	red	green	3	3	4
14	red	red	red	red	red	green	red	red	red	red	1	0	9
15	red	red	red	red	red	green	red	red	red	red	1	0	9
16	yellow	green	red	green	red	green	red	red	red	yellow	3	2	5
17	yellow	red	red	green	yellow	red	green	green	green	green	5	2	3
18	yellow	red	red	red	yellow	green	red	red	green	red	2	2	6
19	yellow	green	red	green	yellow	yellow	green	yellow	green	yellow	4	5	1
$\sum Green$	4	8	0	11	1	9	6	3	7	6	**55**		
$\sum Yellow$	9	0	1	0	7	8	1	3	0	6		**35**	
$\sum Red$	6	11	18	8	11	2	12	13	12	7			**100**