information

MDPI

Article

Monetary Compensation and Private Information Sharing in Augmented Reality Applications

Gilad Taub, Avshalom Elmalech, Noa Aharony and Ariel Rosenfeld *

Information Science Department, Bar-Ilan University, Ramat-Gan 590002, Israel
* Correspondence: ariel.rosenfeld@biu.ac.il; Tel.: +972-35318351

Abstract: This research studied people's responses to requests that ask for accessing their personal information when using augmented reality (AR) technology. AR is a new technology that superimposes digital information onto the real world, creating a unique user experience. As such, AR is often associated with the collection and use of personal information, which may lead to significant privacy concerns. To investigate these potential concerns, we adopted an experimental approach and examined people's actual responses to real-world requests for various types of personal information while using a designated AR application on their personal smartphones. Our results indicate that the majority (57%) of people are willing to share sensitive personal information with an unknown third party without any compensation other than using the application. Moreover, there is variability in the individuals' willingness to allow access to various kinds of personal information. For example, while 75% of participants were open to granting access to their microphone, only 35% of participants agreed to allow access to their contacts. Lastly, monetary compensation is linked with an increased willingness to share personal information. When no compensation was offered, only 35% of the participants agreed to grant access to their contacts, but when a low compensation was offered, 57.5% of the participants agreed. These findings combine to suggest several practical implications for the development and distribution of AR technologies.

Keywords: augmented reality; personal information; information price; security threats

Citation: Taub, G.; Elmalech, A.; Aharony, N.; Rosenfeld, A. Monetary Compensation and Private Information Sharing in Augmented Reality Applications. *Information* **2023**, *14*, 325. https://doi.org/10.3390/info14060325

Academic Editors: Harshvardhan J. Pandit and Andrea Sanna

Received: 23 February 2023
Revised: 24 May 2023
Accepted: 30 May 2023
Published: 8 June 2023

1. Introduction

People constantly generate digital information when using electronic devices. Commercial companies attempt to obtain information about the places we visit, our circle of friends, our daily plans, and more. Prior research has attempted to comprehend how individuals interact with the digital information that they generate, and the findings indicate that most people are either indifferent to or unaware of the potential risks that are associated with sharing their personal information [1–4]. However, if personal information falls into malicious hands, the consequences can be catastrophic [5]. Given the widespread use of smartphones in recent years, there are growing concerns regarding the possible misuse of users' personal information [6–8]. The two major categories of personal information stored on mobile smartphones are personal information (PI) and social information (SI). PI encompasses our recorded voices, captured images, and physical whereabouts. SI encompasses our interactions with others, including messages exchanged, contacts listed, and scheduled events. If any of these types of information are compromised, it can result in negative outcomes.

In the context of mobile apps, reasonable requests for information are those that are necessary for the app to properly function or provide a service to the user. For example, a fitness app might request access to the user's location data to track their outdoor workouts or access to their camera to scan the barcodes of food items. These requests are likely to be accepted by reasonable users because they are directly related to the app's purpose and functionality. On the other hand, unreasonable requests for information are those that

are unnecessary, intrusive, or potentially harmful to the user's privacy. For instance, a gaming app that requests access to the user's contacts or social media accounts without a clear explanation of why such access is needed may not be accepted by a sensible user. Ultimately, it is up to the user to decide whether a request for information by a mobile app is reasonable or not.

AR is a technology that allows users to enhance their perception of the world by overlaying digital information onto their physical environment. AR applications inherently require access to certain features such as cameras, microphones, and GPS location; however, they do not necessarily require access to contacts, calendars, messages, etc. Because AR can run on almost any new mobile phone, users can easily expose their personal information without being aware. As such, this technology poses dangers and threats to users' information. As AR applications have become more ubiquitous, concerns about privacy and data security have also increased. Understanding how people respond to requests for their personal data in AR settings is crucial for improving the design of AR applications and enhancing users' trust in these technologies. By identifying the factors that influence user responses, one can develop strategies to improve the transparency and the user's control over their own personal data, ensuring that AR applications are developed and deployed in a privacy-sensitive manner. While there is scarcely any research investigating how people respond to the personal information access requests made by AR apps, this research aimed to study how users perceive and respond to requests that ask for access to their personal data and how their responses vary depending on the type and sensitivity of the requested information.

The purpose of this study is threefold: first, we empirically demonstrate the extent to which the personal information of people is vulnerable within the context of AR apps; second, we examine how AR app users respond to actual requests seeking access to their personal and social information (PI and SI); and third, we examine how monetary compensation for sharing personal information affects peoples' decisions with respect to sharing their personal information. Next, we provide a brief overview of the prior literature pertaining to AR, privacy, security, and cyber threats in mobile apps. Additionally, we review the use of crowdsourcing for user studies. Then, we introduce this study's research questions and objectives. Next, we describe the conducted experiments pursued by presenting their results and the analysis. Lastly, we discuss the obtained results, draw conclusions, and highlight future work directions.

2. Background

In recent years, there have been increasing concerns about the privacy and security of users' information online, including the information of mobile and AR users. There are several known vulnerabilities in AR applications that could potentially compromise user privacy and security. One such vulnerability is the ability of attackers to manipulate the GPS coordinates used by AR applications to overlay virtual objects onto the real world. By spoofing GPS data, an attacker could trick an AR application into displaying virtual objects in the wrong location, potentially leading to dangerous situations if the virtual objects are mistaken for real ones [9]. Another vulnerability, which more closely relates to our work, involves the use of AR to gather sensitive data such as facial recognition data or location data without the user's knowledge or consent. This could be performed through the use of malicious AR applications or by exploiting vulnerabilities in legitimate AR applications [10]. To mitigate these vulnerabilities, it is important for AR application developers to implement strong security measures, such as encryption and secure communication protocols, to protect user data. Users can also take steps to protect themselves by being cautious about the AR applications that they download and use and by being aware of the potential privacy and security risks associated with these applications. As always, it is important to keep all software up to date with the latest security patches and to practice good cybersecurity conduct to reduce the risk of information being compromised. Nevertheless, there is scarcely any research investigating how people respond to the personal information access

requests that are made by AR apps. The upcoming sections will examine the literature on the use of AR and the privacy concerns, security risks, and cyber threats associated with mobile apps, particularly in the context of their combined usage. In addition, we review the literature related to crowdsourcing and its use in user studies.

2.1. Augmented Reality

AR, as defined by Azuma (1997, p. 355), "allows the user to see the real world, with virtual objects superimposed upon or composited with the real world. Therefore, AR supplements reality, rather than completely replacing it" [11]. The field of AR has seen significant growth in recent years, with numerous studies exploring its potential applications and impact on various areas of research. Here, we will review some of the most relevant and recent studies that have been conducted in the AR field. One area of research that has been greatly impacted by AR technology is education [12–14]. One study that investigated the use of AR in science education found that the incorporation of AR technology led to a significant improvement in students' understanding and engagement with science concepts [15]. Another area of research that has benefited from AR technology is healthcare [16–18]. One study explored the use of AR in surgical procedures, where the technology was used to overlay real-time information on a patient's anatomy during surgery [19]. The authors found that the use of AR technology has led to a significant reduction in surgical errors and improved the accuracy of surgical procedures. The use of AR in marketing has also been extensively studied. Several studies have investigated the effectiveness of AR in promoting consumer engagement and purchase intention in the retail industry [20–22]. The authors found that the use of AR technology led to a significant increase in consumer engagement and purchase intention, indicating the potential of AR in marketing and advertising. In addition to these areas, AR technology has also been applied in various other fields, such as entertainment [23], tourism [24], and architecture [25]. In conclusion, the AR field has seen significant growth in recent years, with numerous studies exploring its potential applications and impact on various areas of research [26]. The studies reviewed above demonstrate the effectiveness and potential of using AR technology in education, healthcare, marketing, entertainment, and other fields. As the technology continues to advance, it is expected that the applications and impact of AR will continue to grow and evolve in new and innovative ways.

Sophisticated AR apps have gained popularity and can now run on standard consumer mobile devices [27]. However, compared with traditional mobile apps, mobile AR apps request access to cameras, microphones, and other sensors, making them more vulnerable to potential risks to users' information [28]. Regrettably, a significant number of users are oblivious to these potential dangers [29,30]. One potential solution to mitigate privacy and security risks involves introducing a new operating system (OS) concept. The Arya platform was created with the aim of reducing the possibility of attacks on mobile phones while utilizing AR applications [31]. This platform, along with the OS, enables the OS to regulate the visual output of AR apps by incorporating an output policy module that alters and governs the AR app outputs in accordance with approved policies [32]. Another solution for addressing privacy and security concerns is to implement a sandbox that restricts the mobile app's access to the file system [33]. This solution minimally affects performance and provides significant benefits in terms of security and privacy. Another solution may be a mechanism that provides an extra layer of privacy protection for safeguarding users' privacy information, particularly when retrieved via cameras and similar devices [34]. This additional protection layer was proven not to impede app functionality. To tackle the physical risks that mobile AR apps pose to users, the PrivacyManager framework was introduced [35]. PrivacyManager utilizes various smartphone features, such as network signal, GPS location, and ambient light, to notify users of potential risks based on predefined rules. For instance, pedestrian users of an AR app may receive a warning that they are about to walk into a road junction.

To the best of our knowledge, very little research has focused on the attitudes of AR mobile app users concerning granting access to different types of information. The purpose of our study is to bridge this gap and empirically investigate users' attitudes concerning granting access to different types of personal information.

2.2. Personal Information Security Threats

The increasing prevalence of smartphones has led to an abundance of personal information being stored on these devices. This section discusses the different types of information that are typically stored on mobile phones and the potential dangers that can arise if this information falls into the wrong hands. One of the most obvious types of information stored on mobile phones is personal contact information; this includes names, phone numbers, email addresses, and even social media profiles. While this information may not seem particularly sensitive, it can be used by hackers or scammers to launch targeted attacks, such as phishing scams or social engineering attacks. Another type of information commonly stored on mobile phones is financial information. This includes credit card numbers, bank account information, and payment apps such as Apple Pay or Google Wallet. If this information is accessed by unauthorized individuals, it can lead to identity theft, fraud, or other financial crimes. Mobile phones also often contain sensitive personal information, such as photos, videos, and messages. This type of information can be particularly damaging if it falls into the wrong hands, as it can be used to embarrass or blackmail individuals. In addition to personal information, mobile phones may also contain business-related information such as emails, classified documents, and calendars; if these devices are not properly secured, it can lead to breaches of corporate data and intellectual property theft. The dangers of this information falling into the wrong hands are significant. Identity theft, financial fraud, and cyberstalking are just a few examples of the risks that individuals face when their personal information is compromised. In addition, businesses can suffer significant financial losses and reputational damage if their sensitive data is exposed. Many apps acquire access to their users' personal information by offering them a premium "free" version of the app in return for access to personal information. Once this "free" app is installed on the mobile device, the user may be asked to grant access to different types of information stored on the device and may be asked to provide a working email address as well. These "free" apps often constitute an invasion of privacy [36,37]. The very existence and adoption of these apps by users highlight the danger inherent in incentive-based mechanisms for information sharing. There is a scarcity of studies that investigate the attitudes and privacy apprehensions of end-users towards AR technologies [28]. Although the limited empirical evidence available suggests that AR raises privacy concerns among users—such as being unintentionally recorded by AR devices as bystanders [38], having their data involuntarily shared, and being subject to surveillance through the use of these devices [39,40]—none of these studies delve into the underlying causes of these concerns. Instead, they use privacy concerns as a precursor for explaining other phenomena, such as elucidating AR usage behavior.

In conclusion, the increasing prevalence of smartphones has led to a wealth of personal and business-related information being stored on these devices. If this information falls into the wrong hands, the consequences can be severe. Therefore, apart from the theoretical contribution of our research, our research has practical implications concerning the security of users' information.

2.3. Price of Information

The topic of how people value their information has been extensively researched in various fields, including economics, psychology, and computer science. In this section, we review some of the most relevant studies that have been conducted in this area. We start by presenting studies that have examined the relationship between demographic characteristics and the price of the information. Research has found that younger people, such as college-age students, are more willing to give up their privacy while using social networks

compared with older social network users [41]. In addition, research has discussed gender differences regarding the use of social networks. For example, one research found that men publish their phone numbers and home addresses more often than women [42]. Other studies have found that women are more prone to actively protect their privacy while using social networks [43]. In addition to the studies above, several studies have focused on understanding how people value their information. For instance, one study investigated how individuals value their personal information, such as their social security number, email address, and credit card number [44]. The authors found that individuals tend to undervalue their personal information and are willing to exchange it for relatively small monetary incentives. Another study that investigated how individuals value their private information in social situations found that individuals tend to overvalue their private information in social situations and are more likely to disclose it to others when they perceive that the information is unique or valuable [45]. A study that investigated how individuals value their online privacy and security found that individuals tend to value their privacy and security more when they perceive that their information is sensitive or could harm them if it was disclosed [46]. A previous research study that investigated people's willingness to share their private information in return for monetary compensation found that, surprisingly, people were willing to trade their information for monetary compensation. Furthermore, the higher the payment that people were offered, the more likely they were to agree to share their personal information [44,47,48].

In light of the previous literature highlighting the monetary value associated with personal information, numerous studies have been proposed to develop automatic systems that evaluate and reward consumers for sharing their personal information with online businesses [49,50]. The concept behind this information system revolves around creating a fair and transparent mechanism that empowers consumers to make informed decisions regarding their personal information. By offering tangible rewards or monetary compensation, online businesses can incentivize individuals to share their data willingly, thus establishing a mutually beneficial relationship between consumers and organizations [51]. To determine the appropriate price for personal information, various factors need to be considered. These may include the sensitivity of the data, the demand for specific types of information, and market dynamics. Overall, the development of an information system for privacy payoff represents a proactive approach to address the growing concerns surrounding personal data usage. By rewarding consumers for sharing their information and by establishing fair compensation mechanisms, this system aims to foster a more balanced and equitable data ecosystem while respecting individual privacy preferences.

In conclusion, the topic of how people value their information has been extensively studied in various fields, including economics, psychology, and computer science. The studies reviewed above demonstrate that individuals tend to undervalue their personal information and that their valuation of information is often influenced by social, situational, and contextual factors. The previous studies mentioned above investigated information pricing behavior in controlled lab experiments. In our study, we investigate this behavior in a simulated real-life situation. Understanding how individuals price their information, especially while using AR technology, is important for developing effective policies and strategies for protecting individuals' privacy and security, particularly in the digital age.

2.4. Using Crowdsourcing Platforms to Elicit Human Behavior

The use of crowdsourcing platforms to test human behavior has become increasingly popular in recent years as it provides researchers with a fast, cost-effective, and diverse pool of participants. Numerous studies have explored the potential of crowdsourcing platforms in various areas of human behavior research, including social psychology, cognitive psychology, and behavioral economics. In this section, we will review some of the most relevant and recent studies that have employed crowdsourcing platforms for testing human behavior. One prominent area of research in which crowdsourcing has been extensively used is social psychology. For instance, the study by Mason and Suri (2012) [52]

demonstrated the effectiveness of using Amazon Mechanical Turk (AMT) to conduct a large-scale study. The authors found that AMT participants were as reliable and valid as those recruited through traditional means, suggesting that crowdsourcing could be a useful tool for conducting social psychology research. Another area of research that has greatly benefited from the use of crowdsourcing platforms is cognitive psychology. In a study by Crump et al. (2013) [53], the researchers used AMT to replicate a well-known cognitive psychology experiment on task switching. The authors found that AMT participants' performance was comparable with that of participants recruited through traditional means, indicating that crowdsourcing could be a valid method for cognitive psychology research. Behavioral economics is another area of research that has extensively utilized crowdsourcing platforms. For example, the study by Horton et al. (2011) [54] used AMT to investigate the role of social influence in charitable giving. The authors found that social influence had a significant impact on the participants' donation behavior, indicating the potential of crowdsourcing platforms for studying social decision making.

In conclusion, the use of crowdsourcing platforms to test human behavior has become increasingly popular in various fields of psychology and economics. The studies reviewed above demonstrate the effectiveness and potential of using crowdsourcing platforms such as AMT as a valid and cost-effective method for conducting research on human behavior. In our study, we used this population as a means to address our research questions.

3. Research Questions and Objectives

Our study addressed the following two research questions:

1. Regarding access requests in AR apps, which types of information are people more/less likely to grant permission to?
2. When people are offered a financial reward for sharing their personal information while using AR apps, is there a linear relationship between the amount of money offered and the responses to the disclosure of personal information? Specifically, when participants are asked to share their personal information, is there a difference in their responses when they are offered no compensation for sharing their information compared to when they are offered high or low compensation for sharing their information?

The objectives of our study are as follows:

1. To assess people's reactions to requests that seek their personal information while using AR apps;
2. To identify which personal information requests people are reluctant to grant access to;
3. To determine the effect of monetary incentives on personal information sharing while using AR apps.

4. Materials and Methods

This study required the creation of computational methods to assess individuals' willingness to allow access to their personal information when using AR apps. To recruit participants, we utilized Amazon Mechanical Turk (AMT), a well-known crowdsourcing platform, for all of the experiments conducted in this study. Participants were required to use their personal smartphones to take part in the experiment, as is typical for workers on such platforms who use their personal computers or mobile phones to complete tasks.

Following an introduction and brief explanation, participants were requested to complete a demographic survey that included questions about their gender, country of residence, and age. Participants were then asked to sign a consent form if they wished to participate in the experiment. To mimic a real-world scenario, participants were informed in the consent form that the objective of the experiment was to test an AR game and that they could leave the experiment whenever they chose to. Note that no personal information was collected during the experiment. After agreeing to the consent form, participants were provided with a link to an assigned AR game to be played on their mobile phones. In the

AR game, each participant was obliged to walk around with their smartphone, searching for objects. The objects were displayed on their smartphones via AR as they moved around the area where they were located. After ten seconds of gameplay, a message popped up on the screen, requesting permission to access personal information stored on the participant's mobile device.

The message shown on the screen and its visual design were intentionally presented in a manner that closely resembled standard access information messages displayed by mobile phones OS. The intention was to create the impression that the AR app was trying to request access to the participant's private information, even though no personal data was actually retrieved. Figure 1 provides an illustration of how these messages were presented.

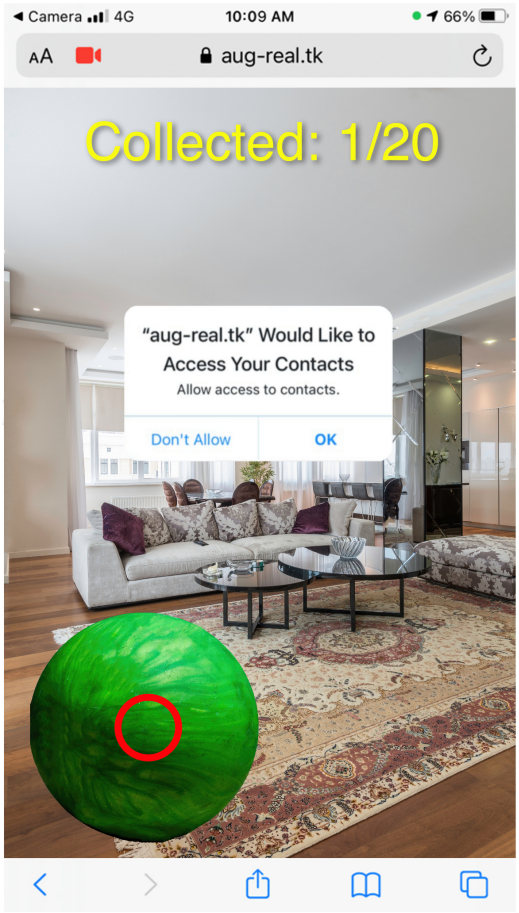

Figure 1. Example of a personal information approval request message (Illustration of the mobile app screen. Pictures of the living room and green ball retrieved from www.pexels.com, accessed on 2 February 2023).

The first objective of this research was to determine the types of permissions that participants were more inclined or disinclined to authorize. To investigate this, our study recruited 600 participants who were divided into six groups, with each group containing 100 individuals. The distinguishing factor among the six groups was the message requesting access to personal information that was presented while participants used the mobile AR app. Each group was exposed to a different type of message requesting permission to access specific personal data, such as text messages, location data, contacts, microphone, photos, and calendar.

The second research question attempted to discover if there was a price tag on personal information. The experiment procedure was almost identical to the previous one. Three groups of participants were asked to interact with the same AR game interface. The only difference between the groups was the compensation offered for sharing their personal

information. For the first group (consisting of 100 participants), no compensation was offered. Participants in the second group (consisting of 40 participants) were offered low compensation (20 cents) for sharing their personal information. Participants in the third group (consisting of 40 participants) were offered high compensation (80 cents) for sharing their personal information. Note that in crowdsourcing platforms, people work for a few cents and thus, 80 cents can be considered a high compensation.

In our analysis, for the descriptive statistics, we use the means and standard deviations. The chi-squared analysis is reported when appropriate.

5. Results

We begin by reporting the demographic data about the participants who took part in the experiment that was designed to examine the attitude of crowdworkers towards sharing different types of information. The demographic characteristics of the crowdworkers who participated in the study are presented in Table 1. It is important to note that as a significant proportion of the participants were residents of the U.S., we only compared the ratios of U.S. and non-U.S. residents among the six experiments. According to the table, there were no substantial dissimilarities between the demographic information of the different groups. Therefore, we can infer that the various groups were a consistent sample population.

Table 1. The demographic data of the participants in our study.

	Mic.	Photos	Cont.	Mess.	Cal.	Loc.	F/χ^2
Age M(SD)	32.47 (10.82)	30.17 (8.82)	30.89 (8.19)	31.79 (10.28)	31.06 (8.58)	32.17 (9.58)	0.85
Female (%)	52%	57%	48%	56%	51%	48%	2.97
U.S. Residence (%)	65%	53%	56%	59%	51%	57%	4.93

The participants' responses to different information-accessing requests are presented in Table 2. It is evident from the table that participants were more inclined to grant access to information that only pertained to them, such as their location, microphone, and pictures. However, they were less willing to grant access to information that could affect their friends if it fell into the wrong hands, such as messages, calendars, and contacts. Moreover, there was a significant discrepancy between the percentage of participants who granted access to their microphone versus their contacts; while 75% of participants granted access to their microphone, only 35% agreed to grant access to their contacts.

Table 2. Participants' reactions to private information requests.

	Mic.	Loc.	Photos	Mess.	Cal.	Cont.
Agreed	75%	68%	67%	53%	44%	35%
Disagreed	25%	32%	33%	47%	56%	65%

The next section addresses the research question dealing with the relationship between the amount of money that is offered for revealing personal information and the decision of whether to reveal such information. As the users were generally reluctant to share their contact list information, we chose to focus on the effect of the reward on their willingness to share this information. We begin by reporting the demographic data about the participants who took part in this portion of the study. Table 3 presents the crowdworkers' demographic characteristics. As demonstrated in the table, no statistically significant differences were found between the demographic data of the different groups.

Table 3. Demographic information of the three groups.

	No Compensation	Low Compensation	High Compensation	F/χ^2
Age, M(SD)	30.89(8.19)	32.23(5.96)	32.08(10.16)	0.85
Female (%)	48%	40%	65%	2.97
U.S. Residence (%)	56%	52.5%	57.5%	0.82

Figure 2 shows the difference in the participants' responses to contact list access requests. As can be observed in the figure, when no reward was offered for giving permission to contacts, only 35% of the participants agreed to grant access to their contacts. When compensation was offered, participants were more willing to grant access to information. While only 40% of the participants agreed to grant access to their contacts for a higher compensation, when a low compensation was offered, 57.5% of the participants agreed. While the differences between the "high compensation" and "low compensation" groups and between the "high compensation" and "no compensation" groups were not found to be statistically significant ($\chi^2 = 1.8011$, $p = 0.18$ and $\chi^2 = 0.1303$, $p = 0.72$, respectively), the difference between the "no compensation" and "low compensation" groups was found to be statistically significant ($\chi^2 = 5.0697$, $p = 0.02*$).

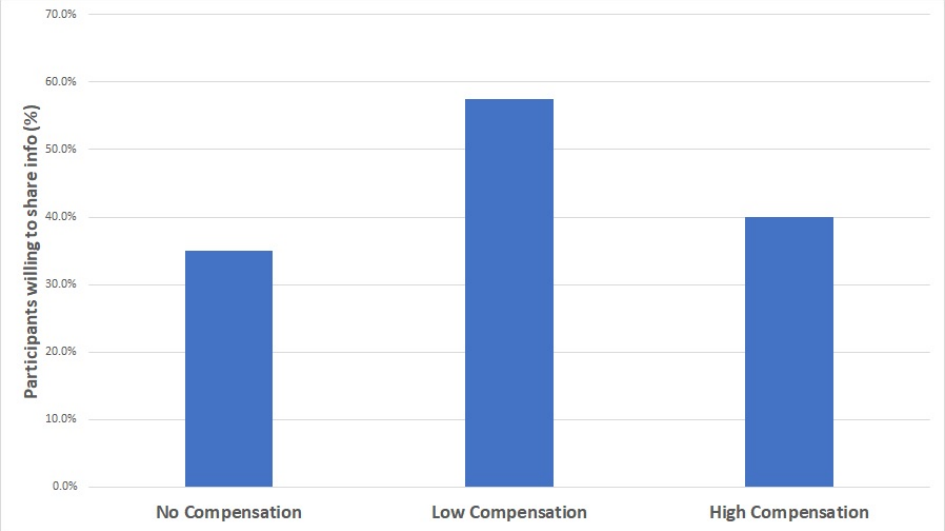

Figure 2. Responses to different compensation values.

6. Discussion

In this study, two critical research questions were addressed. The first inquiry focused on the degree to which individuals allowed AR apps to access various types of personal information. The findings showed that the participants differentiated among the different kinds of information when granting access. They were more open to granting access to their physical personal information, such as their microphone, location, and pictures, than to their social personal information, including messages, calendars, and contacts. These results were unexpected, as previous research has indicated that people regarded messages as less sensitive information than location history [55], leading us to anticipate that participants would prioritize safeguarding their physical information over their social information. Previous research has suggested that it is crucial for individuals to comprehend the purpose behind the request for their personal information [56]. Based on this, we propose the hypothesis that, because AR apps rely on users' physical information, people are more likely to view this information as necessary for the app's proper functioning. In contrast, when a traditional mobile app requests social information, individuals may perceive the request as more legitimate, resulting in a greater willingness to grant access to this type of

information. The second research question examined the effect of monetary compensation on private information sharing. The results of our study indicate that when people are offered low compensation for sharing their information, they are more likely to share it. Surprisingly, when people are offered high compensation, they do not tend to share more information than usual (without compensation). We expected a linear effect, i.e., when the price is higher, more people will be willing to trade their information. A prior study has found that people are willing to share their information when they are offered low compensation; however, this study did not examine what their reaction would be if they were offered different amounts of money [44]. We hypothesize that when people are offered low compensation for their personal information, they tend to believe that their information is not valuable. However, when people are offered high compensation for their information, they understand that their information is valuable and therefore refuse to share it [57]. In the case of a physical object, the value of an object is often determined by external signals, such as demand or price, rather than by the inherent properties or characteristics of the object itself. In other words, the value of an object is largely determined by what others are willing to pay for it rather than by any objective measure of its worth. For example, a rare stamp or coin may have a high value because collectors are willing to pay a premium for it, even though the object itself may have little practical use or intrinsic value. Similarly, the value of a product or service may fluctuate depending on consumer demand, which can be influenced by factors such as advertising, trends, and social influence. Ultimately, the value of an object is not fixed but is subject to external signals that can shift over time, highlighting the importance of considering market dynamics and other external factors when determining the value of an object. In our case, we hypothesize that the value of information is determined by the price offered for this information; we plan to investigate this phenomenon in further research. Overall, the results reported in our work are surprising and contradict the Westin Privacy Segmentation Index [58,59]. The Westin Privacy Segmentation Index categorizes individuals' privacy concerns and attitudes toward personal information. The index aimed to capture different dimensions of privacy preferences and behaviors, including information sensitivity, willingness to disclose personal information, and tolerance for surveillance. The Westin Privacy Segmentation Index consists of three segments: the privacy fundamentalists, the pragmatic, and the unconcerned. In our study, we have found compelling evidence that the decision regarding granting access to personal information is influenced more by the specific type of information being requested and the compensation being offered than the decision being dependent on the user's segment or group. Our research highlights the significant role played by the nature of the information and the incentives provided in shaping individuals' decisions about sharing their personal data. The disparity between our findings and those of Westin could potentially be attributed to the methodology employed in our study. Unlike Westin's approach, which involved asking participants to express their attitudes and sentiments regarding privacy-related questions, our research focused on measuring actual behavioral responses. By examining individuals' real-life actions and decisions concerning the sharing of personal information, our study offers a more tangible and objective perspective on privacy-related behaviors. This divergence in methodology may account for the differences observed in our results when compared with Westin's findings.

7. Conclusions

The focus of this study was to examine how individuals react when asked to grant access to their personal information while using an AR application. The results reinforce the findings reported in previous studies and illustrate the inherent risks to one's personal information. The results of our study indicate that most (57%) of the participants in our study were willing to share sensitive personal information without any compensation other than the use of the application. The results emphasize the need to create appropriate mechanisms that will protect people's privacy and bring this issue to people's attention.

Furthermore, individuals responded in distinct ways to various types of information requests. People were more likely to approve personal information requests, whereas they were reluctant to grant access to social information requests. The variance in individuals' reactions to distinct information requests was significant. For instance, while 75% of participants were willing to grant access to their microphone, only 35% agreed to grant access to their contacts. This result can help privacy educators focus their efforts on explaining the importance of maintaining privacy for certain types of information access requests. Lastly, the results indicated that people are willing to trade their information, even for small monetary compensation. When no compensation was offered, only 35% of the participants agreed to grant access to their contacts; however, when a low compensation was offered, 57.5% of the participants agreed. Thus, regulators and practitioners in this field should intervene to prevent the potential exploitation of people. The findings of this research can have significant implications for the development of AR applications, as well as for policymakers, regulators, and stakeholders who are concerned with data privacy and security in emerging technologies. Ultimately, this research can contribute to the development of a more trustworthy and privacy-preserving AR ecosystem, which can facilitate the widespread adoption and usage of AR technologies in various domains, from entertainment and education to healthcare and industry.

8. Future Work

The present study has provided insight into individuals' willingness to share personal information over mobile phones for low compensation. However, several avenues of future research could expand on these findings and enhance our understanding of the factors that influence people's decisions in this regard. One potential direction for future research is to explore how the individuals' demographics, such as age, sex, and socioeconomic status, influence their willingness to share personal information over their phones. Understanding how these factors interact with compensation could help us develop more targeted strategies to encourage or discourage information sharing, as appropriate. Another area for future research is to investigate how information about the purpose of data collection influences people's decision making. For example, would people be more likely to share personal information if they were informed that it would be used to improve public health outcomes or personalized product recommendations? Alternatively, would people be less likely to share personal information if they knew it would be used for targeted advertising or surveillance purposes? Finally, it would be worthwhile to investigate the psychological factors that underlie people's decisions to share personal information over phones. For example, how do people weigh the benefits of compensation against the potential risks of privacy violations or identity theft? Understanding these underlying motivations could inform the development of more effective communication strategies to encourage responsible data sharing. Overall, the findings of this study provide valuable insights into people's attitudes toward sharing personal information over phones for low compensation. Future research in this area could shed further light on the factors that influence this decision and contribute to the development of more effective policies and guidelines for data privacy and protection.

9. Limitations

We note that the results reported in this study reflect the behavior of the users participating in the AMT crowdsourcing platform. This platform is characterized by short tasks with low-level compensation; thus, they may not be representative of the AR technology user population. In addition, this study did not consider the operating system (iOS/Android) of the users and therefore may have several limitations. Firstly, this study's findings may not be applicable to users of the opposite operating system, and this was not considered in this study. This may limit the generalizability of the results and restrict the broader applicability of this study's findings. Secondly, the research may be biased toward users of a specific operating system, which could impact the validity and reliability

of the results. For example, if this study only recruited iOS users, it may not accurately represent the behavior or preferences of Android users, which could result in misleading conclusions. To generalize our results, additional experiments on different platforms and operating systems are required.

Author Contributions: All authors have contributed equally to this paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

AMT	Amazon Mechanical Turk
AR	Augmented reality
SI	Social information
PI	Personal information
OS	Operating system

References

1. Balebako, R.; Jung, J.; Lu, W.; Cranor, L.F.; Nguyen, C. "Little brothers watching you" raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24–26 July 2013; pp. 1–11. [CrossRef]
2. Liu, R.; Cao, J.; Yang, L. Smartphone privacy in mobile computing: Issues, methods and systems. *Inf. Media Technol.* **2015**, *10*, 281–293. [CrossRef]
3. Quermann, N.; Degeling, M. Data sharing in mobile apps—User privacy expectations in Europe. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 107–119. [CrossRef]
4. Waldman, A.E. Cognitive biases, dark patterns, and the 'privacy paradox'. *Curr. Opin. Psychol.* **2020**, *31*, 105–109. [CrossRef] [PubMed]
5. Shklovski, I.; Mainwaring, S.D.; Skúladóttir, H.H.; Borgthorsson, H. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 2347–2356. [CrossRef]
6. Degirmenci, K. Mobile users' information privacy concerns and the role of app permission requests. *Int. J. Inf. Manag.* **2020**, *50*, 261–272. [CrossRef]
7. Kununka, S.; Mehandjiev, N.; Sampaio, P. A comparative study of Android and iOS mobile applications' data handling practices versus compliance to privacy policy. In Proceedings of the IFIP International Summer School on Privacy and Identity Management, Ispra, Italy, 4–8 September 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 301–313.
8. Wang, T.; Duong, T.D.; Chen, C.C. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *Int. J. Inf. Manag.* **2016**, *36*, 531–542. [CrossRef]
9. Zeng, K.C.; Shu, Y.; Liu, S.; Dou, Y.; Yang, Y. A practical GPS location spoofing attack in road navigation scenario. In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, Sonoma, CA, USA, 21–22 February 2017; pp. 85–90.
10. CVE-2022-30717. Samsung Mobile Security. CVE. Available online: https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=6 (accessed on 1 February 2023).
11. Azuma, R.T. A Survey of Augmented Reality. *Presence Teleoperators Virtual Environ.* **1997**, *6*, 355–385. [CrossRef]
12. Köse, H.; Güner-Yildiz, N. Augmented reality (AR) as a learning material in special needs education. *Educ. Inf. Technol.* **2021**, *26*, 1921–1936. [CrossRef]
13. Lohre, R.; Wang, J.C.; Lewandrowski, K.U.; Goel, D.P. Virtual reality in spinal endoscopy: A paradigm shift in education to support spine surgeons. *J. Spine Surg.* **2020**, *6*, S208. [CrossRef] [PubMed]
14. Subhashini, P.; Siddiqua, R.; Keerthana, A.; Pavani, P. Augmented reality in education. *J. Inf. Technol.* **2020**, *2*, 221–227. [CrossRef]
15. Dunleavy, M.; Dede, C.; Mitchell, R. Affordances and limitations of immersive participatory augmented reality simulations for teaching and learning. *J. Sci. Educ. Technol.* **2009**, *18*, 7–22. [CrossRef]
16. Ong, S.K.; Zhao, M.; Nee, A.Y.C. Augmented Reality-Assisted Healthcare Exercising Systems. In *Springer Handbook of Augmented Reality*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 743–763. [CrossRef]
17. Berciu, A.G.; Dulf, E.H.; Stefan, I.A. Flexible Augmented Reality-Based Health Solution for Medication Weight Establishment. *Processes* **2022**, *10*, 219. [CrossRef]
18. Innocente, C.; Ulrich, L.; Moos, S.; Vezzetti, E. Augmented Reality: Mapping Methods and Tools for Enhancing the Human Role in Healthcare HMI. *Appl. Sci.* **2022**, *12*, 4295. [CrossRef]

19. Shuhaiber, J.H. Augmented reality in surgery. *Arch. Surg.* **2004**, *139*, 170–174. [CrossRef]
20. Scholz, J.; Smith, A.N. Augmented reality: Designing immersive experiences that maximize consumer engagement. *Bus. Horizons* **2016**, *59*, 149–161. [CrossRef]
21. Arghashi, V.; Yuksel, C.A. Interactivity, Inspiration, and Perceived Usefulness! How retailers' AR-apps improve consumer engagement through flow. *J. Retail. Consum. Serv.* **2022**, *64*, 102756. [CrossRef]
22. Jiang, Z.; Seock, Y.K.; Lyu, J. Does Augmented Reality really engage consumers? Exploring AR driven consumer engagement. *Int. Text. Appar. Assoc. Annu. Conf. Proc.* **2022**, *78*, 1–4. [CrossRef]
23. Hung, S.W.; Chang, C.W.; Ma, Y.C. A new reality: Exploring continuance intention to use mobile augmented reality for entertainment purposes. *Technol. Soc.* **2021**, *67*, 101757. [CrossRef]
24. Wei, W. Research progress on virtual reality (VR) and augmented reality (AR) in tourism and hospitality: A critical review of publications from 2000 to 2018. *J. Hosp. Tour. Technol.* **2019**, *10*, 539–570. [CrossRef]
25. Song, Y.; Koeck, R.; Luo, S. Review and analysis of augmented reality (AR) literature for digital fabrication in architecture. *Autom. Constr.* **2021**, *128*, 103762. [CrossRef]
26. Shevchuk, R.; Tykhiy, R.; Melnyk, A.; Karpinski, M.; Owedyk, J.; Yurchyshyn, T. Cyber-physical System for Dynamic Annotating Real-world Objects Using Augmented Reality. In Proceedings of the 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 26–28 September 2022; pp. 392–395. [CrossRef]
27. Mendigochea, P. WebAR: Creating Augmented Reality Experiences on Smart Glasses and Mobile Device Browsers. In Proceedings of the ACM SIGGRAPH 2017 Studio, Los Angeles, CA, USA, 30 July–3 August 2017; SIGGRAPH' 17; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1–2. [CrossRef]
28. Harborth, D.; Pape, S. Investigating privacy concerns related to mobile augmented reality apps—A vignette based online experiment. *Comput. Hum. Behav.* **2021**, *122*, 106833. [CrossRef]
29. Roesner, F.; Kohno, T.; Molnar, D. Security and privacy for augmented reality systems. *Commun. ACM* **2014**, *57*, 88–96. [CrossRef]
30. Braghin, C.; Del Vecchio, M. Is Pokémon GO watching you? A survey on the Privacy-awareness of Location-based Apps' users. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 4–8 July 2017; Volume 2, pp. 164–169. [CrossRef]
31. Lebeck, K.; Ruth, K.; Kohno, T.; Roesner, F. Arya: Operating system support for securely augmenting reality. *IEEE Secur. Priv.* **2018**, *16*, 44–53. [CrossRef]
32. Lebeck, K.; Kohno, T.; Roesner, F. How to safely augment reality: Challenges and directions. In Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, St. Augustine, FL, USA, 23–24 February 2016; pp. 45–50. [CrossRef]
33. Thompson, C.; Wagner, D. Securing recognizers for rich video applications. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Vienna, Austria, 24 October 2016; pp. 53–62. [CrossRef]
34. Jana, S.; Narayanan, A.; Shmatikov, V. A scanner darkly: Protecting user privacy from perceptual applications. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 349–363. [CrossRef]
35. Lehman, S.M.; Tan, C.C. PrivacyManager: An access control framework for mobile augmented reality applications. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 1–9. [CrossRef]
36. Brandtzaeg, P.B.; Pultier, A.; Moen, G.M. Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. *Soc. Sci. Comput. Rev.* **2019**, *37*, 466–488. [CrossRef]
37. Wottrich, V.M.; van Reijmersdal, E.A.; Smit, E.G. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decis. Support Syst.* **2018**, *106*, 44–52. [CrossRef]
38. Denning, T.; Dehlawi, Z.; Kohno, T. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 2377–2386. [CrossRef]
39. Dacko, S.G. Enabling smart retail settings via mobile augmented reality shopping apps. *Technol. Forecast. Soc. Chang.* **2017**, *124*, 243–256. [CrossRef]
40. Rauschnabel, P.A.; He, J.; Ro, Y.K. Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *J. Bus. Res.* **2018**, *92*, 374–384. [CrossRef]
41. Tufekci, Z. Can you see me now? Audience and disclosure regulation in online social network sites. *Bull. Sci. Technol. Soc.* **2008**, *28*, 20–36. [CrossRef]
42. Fogel, J.; Nehmad, E. Internet social network communities: Risk taking, trust, and privacy concerns. *Comput. Hum. Behav.* **2009**, *25*, 153–160. [CrossRef]
43. Hoy, M.G.; Milne, G. Gender differences in privacy-related measures for young adult Facebook users. *J. Interact. Advert.* **2010**, *10*, 28–45. [CrossRef]
44. Grossklags, J.; Acquisti, A. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In Proceedings of the WEIS. 2007; pp. 1–22. Available online: https://econinfosec.org/archive/weis2007/program.htm (accessed on 8 May 2023).
45. Xu, H.; Teo, H.H.; Tan, B.C.; Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *J. Manag. Inf. Syst.* **2009**, *26*, 135–174. [CrossRef]

46. Xu, H.; Luo, X.R.; Carroll, J.M.; Rosson, M.B. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decis. Support Syst.* **2011**, *51*, 42–52. [CrossRef]
47. Benndorf, V.; Normann, H.T. The willingness to sell personal data. *Scand. J. Econ.* **2018**, *120*, 1260–1278. [CrossRef]
48. Pugnetti, C.; Elmer, S. Self-assessment of driving style and the willingness to share personal information. *J. Risk Financ. Manag.* **2020**, *13*, 53. [CrossRef]
49. Mayle, A.; Bidoki, N.H.; Masnadi, S.; Boeloeni, L.; Turgut, D. Investigating the Value of Privacy within the Internet of Things. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6. [CrossRef]
50. Oh, H.; Park, S.; Lee, G.M.; Choi, J.K.; Noh, S. Competitive data trading model with privacy valuation for multiple stakeholders in IoT data markets. *IEEE Internet Things J.* **2020**, *7*, 3623–3639. [CrossRef]
51. Yassine, A.; Shirehjini, A.A.N.; Shirmohammadi, S.; Tran, T.T. Knowledge-empowered agent information system for privacy payoff in eCommerce. *Knowl. Inf. Syst.* **2012**, *32*, 445–473. [CrossRef]
52. Mason, W.; Suri, S. Conducting behavioral research on Amazon's Mechanical Turk. *Behav. Res. Methods* **2012**, *44*, 1–23. [CrossRef]
53. Crump, M.J.; McDonnell, J.V.; Gureckis, T.M. Evaluating Amazon's Mechanical Turk as a tool for experimental behavioral research. *PLoS ONE* **2013**, *8*, e57410. [CrossRef] [PubMed]
54. Horton, J.J.; Rand, D.G.; Zeckhauser, R.J. The online laboratory: Conducting experiments in a real labor market. *Exp. Econ.* **2011**, *14*, 399–425. [CrossRef]
55. Staiano, J.; Oliver, N.; Lepri, B.; de Oliveira, R.; Caraviello, M.; Sebe, N. Money walks: A human-centric study on the economics of personal mobile data. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014; pp. 583–594. [CrossRef]
56. Consolvo, S.; Smith, I.E.; Matthews, T.; LaMarca, A.; Tabert, J.; Powledge, P. Location disclosure to social relations: Why, when, & what people want to share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, OR, USA, 2–7 April 2005; pp. 81–90. [CrossRef]
57. Kardes, F.R.; Cronley, M.L.; Kellaris, J.J.; Posavac, S.S. The Role of Selective Information Processing in Price-Quality Inference. *J. Consum. Res.* **2004**, *31*, 368–374. [CrossRef]
58. Westin, A.F.; Maurici, D. *E-Commerce & Privacy: What Net Users Want*; Privacy & American Business: Hackensack, NJ, USA, 1998.
59. Kumaraguru, P.; Cranor, L.F. Privacy Indexes: A Survey of Westin's Studies. pp. 2–3. Available online: https://kilthub.cmu.edu/articles/journal_contribution/Privacy_indexes_a_survey_of_Westin_s_studies/66254062005 (accessed on 8 May 2023).