Privacy Perceptions Across the XR Spectrum: An Extended Reality Cross-Platform Comparative Analysis of A Virtual House Tour

Chris Warin
Institute of Computer Science
University of Göttingen
warin@cs.uni-goettingen.de

Viktoriya Pak
Institute of Computer Science
University of Göttingen
viktoriya.pak@stud.uni-goettingen.de

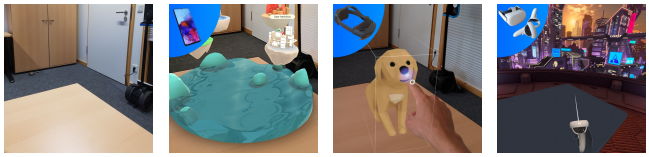
Delphine Reinhardt
Institute of Computer Science
Campus Institute Data Science
University of Göttingen
reinhardt@cs.uni-goettingen.de

Abstract

Extended Reality (XR) devices are becoming available in all shapes and forms, ranging from *Augmented Reality* (AR) to *Mixed Reality* (MR) to *Virtual Reality* (VR). They are foreseen to be the backbone of the Metaverse, which is expected to increasingly lead toward more interconnected XR experiences in the future. However, these devices include many sensors that collect sensitive data about users and their surroundings, thus posing threats to their privacy. Until now, research on how users perceive these threats has rather focused on either *Mobile Augmented Reality* (MAR), MR, or VR. Still, adopting a global vision including all these technologies, i.e., XR, is necessary to understand the potential differences in privacy between users that future cross-platform experiences may cause. This understanding is needed to bring usable *Privacy-Enhancing Technologies* (PETs) to XR users. In this paper, we therefore consider different XR technologies together, and analyze users' related privacy perceptions. By doing so, we observe differences and similarities between each of these technologies by comparing them against each other. In our study, 20 participants have visited a virtual house guided by a real estate agent, with a cross-platform application that we developed for (1) Android (MAR), (2) Microsoft Hololens (MR), and (3) Meta Quest 2 (VR). They tested our application with two of these devices. We then conducted a semi-structured interview to gather comparisons and insights on their experience with both technologies, including permission requests, sensor data collection, and privacy perceptions. Our findings suggest that our participants are more concerned about MAR and MR than VR. We found they were less aware about the use of camera and eye-tracking data than microphone data in the context of our application. In addition, half of our participants were more concerned about XR than more common technologies (i.e., computers, smartphones), despite overall low concerns on XR and low awareness on biometric data sensitivity. These insights underline aspects that must further be developed to raise XR users' awareness and help them control their privacy better, such as adapted permissions to track surfaces in XR.

Keywords

Privacy Perceptions, Extended Reality, User Study



(a) Reality **(b) MAR Android** **(c) MR HoloLens 2** **(d) VR Quest 2**

Figure 1: Demonstration of different XR technologies (devices in top-left corner). MAR projects virtual content on top of reality through the screen of the smartphone; MR enables eye and hand interactions with holograms projected through transparent lenses; VR immerses the user in a virtual world by isolating the visual sense with an opaque HMD.

1 Introduction

XR, a superset of AR, MR and VR, is expanding fast. AR devices project 3D content on top of a user's perception of the real world, typically through a smartphone screen (i.e., MAR) or a *Head-Mounted Display* (HMD), such as the recently released Apple Vision Pro. MAR use cases include popular mobile games (e.g., Pokemon Go), or features in existing tools (e.g., Google Maps, Google Translate), totaling hundreds of millions of downloads on app stores [1]. MR, while traditionally considered as a middle ground between AR and VR [2], grew to be considered as a more immersive and interactive type of AR, enabling hand interactions with 3D holograms through transparent HMDs (as opposed to 2D screen interactions on smartphone/tabled-based MAR) [3]. MR use cases have recently grown in the medical, education and engineering fields [4]. Lastly, VR fully isolates the user in a virtual world, through the use of an opaque headset. VR has also greatly expanded in the last decade, with a worldwide cumulative installed base of 14 million headsets in 2020 [5]. Examples of MAR, MR and VR are shown in Fig. 1. Furthermore, joint efforts made by leader tech companies are currently focused on building the Metaverse, a popular concept aiming to embed XR into the real world, reaching for more interconnected, immersive, and hybrid experiences in virtual worlds, where people will be able to interact, play, work and learn together [6].

Despite the excitement and potential of these new technologies, privacy concerns have also risen in the past decade [7]. All XR devices contain numerous sensors, e.g., cameras, microphones, gyroscopes, accelerometers, and eye trackers. These sensors are required for the functioning of the technologies, but represent risks for users' privacy, as discussed for each technology in isolation [7].

Proceedings on Privacy Enhancing Technologies 2025(1), 150–168

https://doi.org/10.56553/popets-2025-0009

Table 1: Overview of related work in user privacy perceptions in XR. "|" separates samples, L: Lab, F: Field, O: Online.

Paper	Year	Technology			Main addressed topics							Demographics				Methodology				
		MAR	AR/MR	VR	Authentication	Privacy Policies	Data Collection	Access Control	Bystanders	Social Behaviour	Priv. Ment. Model	Users	Bystanders	Developers	Experts	Interviews	Experiment	Focus groups	Think Aloud	Questionnaire
Denning et al. [8]	2014		✓				✓		✓		✓		31			F				
Lebeck et al. [9]	2018		✓						✓	✓	✓	22				L	L			
Rauschnabel et al. [10]	2018		✓						✓		✓	285|21				O				O
Adams et al. [11]	2018			✓		✓	✓	✓				10		10		O				
Maloney et al. [12]	2020			✓						✓	✓	30				O				
Cowan et al. [13]	2021	✓				✓	✓				✓	251|165								O
Harborth and Pape [14]	2021	✓					✓	✓			✓	1100					O			
Abraham et al. [15]	2022	✓	✓	✓		✓	✓		✓	✓					5|4|4			L		
Sykownik et al. [16]	2022			✓						✓	✓	126								O
O'Hagan et al. [17]	2022		✓				✓		✓		✓		102							O
O'Hagan et al. [18]	2023			✓					✓	✓	✓	16					L		L	
Gallardo et al. [19]	2023		✓				✓		✓	✓	✓	21				O				
Li et al. [20]	2023			✓	✓							24					L			L
Hadan et al. [21]	2024	✓	✓	✓								464								O
Ours	**2024**	✓	✓	✓			✓	✓	✓	✓	✓	**20**				**L**	**L**			

Still, works on the privacy perceptions of XR users remain scarce. Until now, AR, MR, and VR have rather been considered as standalone technologies [22]. However, XR increasingly becomes cross-platform and interconnected, and it is unclear how users perceive these new environments. Future cross-platform experiences where users interact with different devices may introduce new privacy threats, or differences in privacy between users. Assume a user who connects to a social network through their VR headset, which enables body tracking through the poses (i.e., positions and rotations) of the headset and hand controllers. Such a user could potentially reveal more information about themselves (through, e.g., their gait) than a MAR user would with a smartphone without body tracking. To address these possibilities, it is important not to simply research each XR variant individually, but to compare them to each other in a practical setting. Thus, to assist future XR users in protecting their privacy, more research is needed, with the consideration of XR as a whole rather than as the sum of its components. To this end, we focus on studying and comparing XR privacy concerns across different XR platforms and devices. Understanding these concerns is important to provide PETs that match the users' needs and help them better control their privacy in XR environments.

We sum up the contributions of this paper in the following:

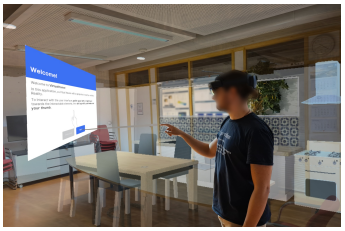
- We have conducted a qualitative lab study (n=20) on global XR privacy perceptions, gathering users' insights on different XR devices with the same cross-platform application that we have implemented, thus enabling qualitative analysis from both a within-subjects and between-subjects perspective. With our cross-platform XR application, which allows multi-user interactions in real-time for MAR, MR and VR, participants experienced a virtual house tour, guided by a real estate agent.
- We provide new findings on XR privacy perceptions, suggesting that our participants are in general more concerned about MAR (seen as an extension of smartphones), mixed about MR (the least known technology), and less about VR (sometimes seen as a gaming-only device). In addition, half of our participants are more concerned about XR than more common technologies (i.e., computers, smartphones), despite overall low concerns on XR and low awareness on biometric data sensitivity. In particular, we observe a low degree of awareness regarding the use of camera data in the context of our applications, and a lack of understanding about the need for cameras in XR.
- We compare the privacy perceptions of users on XR sensor data collection to more established technologies, i.e., smartphone sensor data collection.
- We propose future research directions based on our results, including the development of more adapted, XR specific permission requests, and materials to better explain the use of cameras in XR, in order to raise user awareness.

This paper is structured as follows. After describing related work (Sec. 2), we present our methodology, including our cross-platform XR application (Sec. 3). Our results are described in Sec. 4, and discussed in Sec. 5. Finally, we conclude this work with an outlook of possible future research directions for privacy in XR (Sec. 6).

2 Related Work

Privacy threats in XR have been discussed in literature, and systematised in literature reviews, such as [7]. In particular, privacy risks related to biometric, behavioural, and spatial data have been growing topics of interest in privacy research in recent years. Works on eye-tracking in VR have identified privacy threats and proposed novel privacy-preserving solutions [23, 24, 25, 26], while works on body motion data collection have shown the possibility of, e.g., accurate user (re)identification [27, 28, 29, 30, 31, 32, 33], or of key-logging user-typed text [34]). In the field of AR, Liebers et al. have

(a) Samsung Galaxy S20+ (MAR)



(b) Microsoft HoloLens 2 (MR)

(c) Meta Quest 2 (VR)

Figure 2: Overview of our study setup with three XR devices. The virtual house is anchored to the physical room, so that moving in the physical room results in moving in the virtual house. In MAR, the virtual house and the real estate agent's avatar are seen through the smartphone screen (2a). In MR, transparent 3D holograms are shown through the lenses, with some elements overlapping with real-life objects, such as the virtual table and the real table (2b). The user interface (e.g., tutorials), is shown in the form of floating panels. Full immersion is done in VR, where moving is primarily done by using the controllers (2c).

analysed the impact of hand tracking in AR [35]. Finally, De Guzman et al. have explored the privacy risks posed by the collection of 3D/spatial data in modern MR devices, such as [36, 37]. In this paper, we do not directly focus on these privacy threats, but focus on users' privacy perceptions of the underlying XR devices instead.

We provide an overview of seminal works that have analysed users' privacy perceptions in AR, MR, and VR in Tab. 1. To this end, we group HMD-based AR and MR together. The reason for this grouping is that their distinction is inconsistent [3]. For example, the Microsoft Hololens is considered as an AR device (e.g., in [9]), but also as an MR device (e.g., in [7]). Thus, we separate smartphone/tablet-based MAR from HMD-based AR, which we group with MR. In our study, we qualify the Hololens as MR.

User studies prior to 2020 [8, 9, 10, 11] did not consider the risks of biometric, behavioural, and spatial data. Recent works now consider these new threats, e.g., self-disclosure in social VR [12], privacy concerns on MAR face filters [13], and insights from XR experts [15]. Still, more qualitative data is needed from XR end users to obtain an understanding on each XR technology. Thus, we aim to observe whether XR user concerns on data collection have evolved to consider biometric and behavioural privacy threats.

Furthermore, some of the concerns discussed in these studies might have evolved since, thanks to the implementation of privacy-enhancing technologies into XR consumer devices. For example, the authors of [11] noted that at the time (2018), VR applications lacked permission mechanisms. This has since evolved, as permission-based access control mechanisms are now implemented in all the devices that we used in our study. Observing users' perceptions when confronted with such mechanisms is therefore relevant to determine whether they contribute to user privacy awareness.

Lastly, most user studies on privacy perceptions [8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20], focus on a sole technology in XR, i.e., either MAR, HMD-based AR/MR, or VR. To the best of our knowledge, only two studies [15, 21] gather privacy and security insights on XR as a whole. While it can be necessary to understand each XR technology separately; we now enter an era of interconnected, cross-platform XR experiences, with widespread industry adoption of open standards [38]. Therefore, more work is required with a global vision for XR in mind.

In summary, our contributions are novel because we (1) consider global XR privacy perceptions, (2) study user awareness on XR data collection, and (3) compare user perceptions between each XR variant, on various dimensions including access control mechanisms.

3 Methodology

3.1 Research Questions

Our overarching objective is to bring usable tools to users in order to help them better control their privacy in XR environments. For this, we first need to understand the current privacy perceptions of users regarding the different XR devices and the underlying data. Furthermore, research in usable privacy and security advocates for privacy systems to bring more awareness to users, to support privacy [39, 40]. Therefore, our study needs to measure the existing awareness of users on XR devices. From these requirements, we derive the following research questions:

RQ1. *What are users' privacy perceptions on AR, MR and VR devices and their related data collection aspects?*

RQ2. *What is the degree of awareness of users regarding the sensitivity of the data collected by XR devices?*

To answer these research questions, we designed our user study in a way that would let us follow the experience of our participants, from their reaction to permission requests as an entry point in privacy discussion, to their underlying awareness and privacy perceptions. In the following, we describe the methods used in the design, conduction, and analysis of our user study.

3.2 Scenario

We have designed a scenario that would help us answer our research questions, while not priming our participants by telling them the goal of the study. The scenario is as follows: The participant tries our new virtual house tour application on a given XR device. In this application, they visit a house for sale, guided by a real estate agent named Hannah Schneider (chosen by combining common first and last names in the country the study was conducted in) who is present in the house in the form of a 3D avatar. The real estate agent presents the different rooms to the participant, who can freely move in the house and ask questions, like in a real-life house visit. At the end of the visit, the participant quits the application and repeats the process a second time with a different XR device. The virtual house is shown in Fig. 2 for all used XR devices. The real estate agent is played by a researcher located in another room.

To answer our research questions, our scenario needed to give a primary task to the participants which was not directly linked to privacy (i.e., virtually visiting a house for sale), while enabling data collection through the various XR devices during the experiment. Although interacting with a real estate agent is not something one might do often, the context of following and answering the agent during a visit enables the possibility to give tasks to the participants, without giving them precise indications. Moreover, we argue that the choice of this scenario fits the goal of this study, which is about privacy perceptions on data collection aspects, and not about privacy perceptions on virtual social interactions. Thus, the real estate agent gave tasks to the participants during the experiment to justify that data could be collected from their actions.

The first task is to walk in the virtual space. For this, the real estate agent tells the participant "Please do not hesitate to follow me around the house or to move freely, so you can get a better opinion". This generates body movement data seamlessly.

The second task is to orally communicate with the real estate agent. This is possible through the real-time voice chat functionality of the application. This functionality is automatically enabled when the participant connects to the virtual house from the application's main menu; i.e., the participant hears the real estate agent upon connecting to the virtual room. A visual indicator shows whether the participant's microphone is enabled or muted.

Lastly, the third task is for the participant to decide whether they agree to disclose their full name publicly to the real estate agent. This was done in the form of a suggestion, so that we could respect the wish of the participant to remain anonymous if they desired so. If they agree, the participant's full name is displayed on a floating card above their head, as seen in Fig. 2a. The full name of the participant is already present in the application at the moment they are encouraged to disclose it. Instead of having them enter it themselves, we ask them to write it on a piece of paper before testing the application, and enter the name from the server side for the duration of the experiment. The piece of paper and name information are discarded as soon as the application is quit. This method lets us observe the participants' behaviour without the influencing factor of having to type in their name themselves through different XR input methods (e.g., holographic keyboard), which may be repetitive or annoying due to the limited usability of these methods. We justify this approach in the scenario, by telling them that we create a user account with their name for the study, with their permission. While not typing their name themselves can impact their perception of this data type, participants still need to agree to disclose their name first before writing it, because of the way we designed the study. This task focuses on the self-disclosure aspect of the participants' behaviour rather than their perception of their name. We therefore do not consider this as a limitation.

3.3 XR Devices Specifications

For our user study, we chose one popular device from each XR technology: A Samsung Galaxy S20+ for MAR, a Microsoft Hololens 2 for MR, and a Meta Quest 2 for VR. Although these devices have different interfaces, we chose to compare them to illustrate the diversity of XR experiences that users may experience in the future. We provide the technical specifications of these devices in Tab. 2, including their tracking capabilities and the main privacy implications that have been identified in research. In the remainder of this paper, we use these identified privacy risks as ground truth to be compared with the privacy perceptions of our participants.

Table 2: Technical specifications, data collection practices, and privacy implications of the XR devices used in our study.

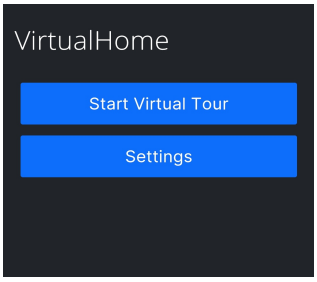
Device		Samsung Galaxy S20+ (MAR)	Microsoft Hololens 2 (MR)	Meta Quest 2 (VR)
Sensors	OS	Android 13	Windows 10 Holo.	Android 10
	Cameras	Front, Back	4 Front, 2 Inner IR	4 Front (grayscale)
	Microphone	✓	✓	✓
	Accelerometer	✓	✓	✓
	Gyroscope	✓	✓	✓
	GPS	✓		
Tracking	Environment	✓[2]	✓	✓
	Face	✓[2]		
	Hands	✓[2]	✓	✓(opt-in)
	Controllers			✓
	6DoF[1] Head		✓	✓
	Eye-Tracking		✓	
Privacy Implications	Bystanders	[37, 41, 42]	[8, 17, 43]	[18, 44]
	Spatial Inference	[36]	[36]	
	Shoulder Surfing	[45]		[46]
	Raw Sensor Access	[47]		
	Unlawful Sensor Use	[48]		
	Face Track. Sensitiv.	[13]		
	Eye Track. Sensitiv.		[23, 24, 25, 26]	
	Body Track. Sensitiv.			[29, 30, 31, 32, 33]

[1] 6 Degrees of Freedom, i.e., full position and rotation tracking.
[2] Requires AR Framework (e.g., Google ARCore).

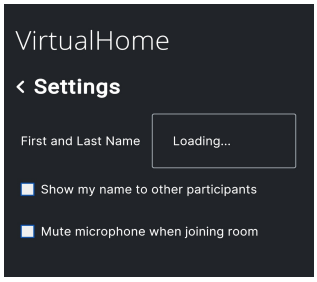
3.4 Cross-platform XR Application

3.4.1 Application Specification. With the industry's quick adoption of open standards like OpenXR [38, 49], we expect future XR apps to increasingly support multiple platforms. With this in mind, we developed a cross-platform XR application for our study and scenario. We chose to develop our application with the Unity3D engine, as it supports a wide range of devices and vendors, making it ideal for cross-platform applications. Unity notably supports different plugins that facilitate XR functionalities, including ARCore for Android, and the OpenXR plugin for the Meta Quest 2 and Hololens 2. In addition, we have used a homemade Unity extension to facilitate the creation of responsive *User Interface*s (UIs) in XR. This allows us to create and use the same UIs for each variant of the application, resulting in all variants looking and behaving as similarly as possible. Thanks to the cross-platform nature of the application and the responsive UIs, we can reduce the varying parameters between each variant to the XR experience itself, as the virtual world, graphics and UIs are the same for all variants.

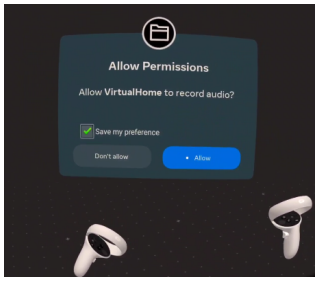
We opted for a cross-platform XR application for two reasons. First, developing for multiple devices follows the vision of the Metaverse, which propels interconnected experiences across different devices. For example, users could join the same virtual call using a VR headset or with MR glasses, thus sharing the same experience through different devices, each having their own unique characteristics. We believe that following this vision—which the XR industry embraces—is necessary for privacy research to stay up to date and for mitigating new privacy risks, while the Metaverse is still being modelled. The second reason for a cross-platform application is



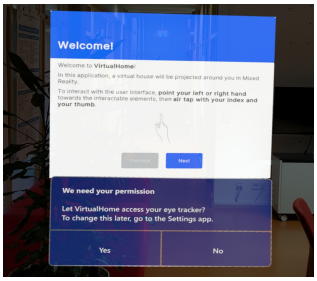
(a) Main menu of the application



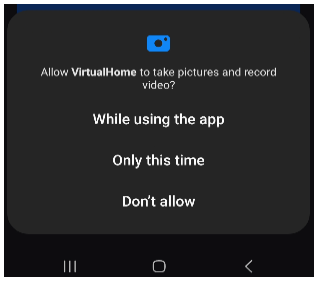
(b) Settings of the application



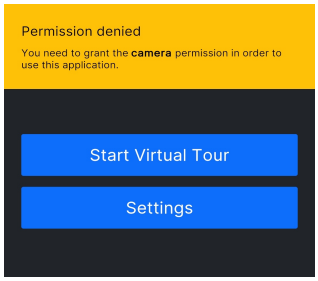
(c) Microphone permission (VR)



(d) Eye tracker permission (MR)



(e) Camera permission (MAR)



(f) Camera permission denied alert

Figure 3: Screenshots of our VirtualHome application. From the main menu (3a), clicking "Settings" leads to the settings page (3b). Clicking "Start Virtual Tour" triggers the permission requests on the respective device (3c, 3d, 3e) then starts the virtual tour upon granting permissions. Refusing the permission(s) shows an alert (3f).

to provide users with an experience that is as similar as possible between each XR variant. Thus, having similar—or identical when possible—UIs and functionalities across each XR variant enables us to give the same scenario and same tasks to our participants. This reduces the differences between experiences for aspects other than privacy perceptions, and helps us point out differences in privacy perceptions between each XR variant more easily.

3.4.2 Application Design. Our application uses the same UI for all variants, albeit adapted responsively for each device. When starting the application on any device, a tutorial popup appeared, and instructed the participant how to interact with the UI and how to move, depending on the device they were using (a tutorial on the MR variant of the app can be seen in Fig. 2b). We opted for in-app tutorials to have a consistent explanation for every participant.

Once the tutorial popup was closed, the main menu of the application appeared (Fig. 3a). The menu contained two entries: a "Start Virtual Tour" button, which connected the participant to the virtual house, and a "Settings" button, which opened a settings page (Fig. 3b). On this page, participants could define privacy settings. A text field allowed them to see their full name, which we entered in real-time from the application server once they joined the virtual room. Prior to the participant's connection to the room, the text field indicated "Loading...". Participants could choose whether their full name should be shown to other users (i.e., the real estate agent) by checking the associated checkbox (by default unchecked). A second checkbox determined whether the participant's microphone would be enabled or muted upon connecting to the virtual house.

If the participant pressed the "Start Virtual Tour" button, they were prompted with permission requests by the device's *Operating System* (OS). All three variants requested access to the microphone (e.g., Fig. 3c). The MR variant running on the Microsoft Hololens additionally requested access to the device's eye tracker (Fig. 3d), despite not actually using it. Interestingly, no camera permissions were necessary from the user to run the application for the MR and VR variants. This is because camera frames are processed by the device to calculate planes and spatial data. These data are fed to the OpenXR API, which returns high-level information to the app. Thus, the app never accesses the camera and does not require permission to it. However, this was not the case for the MAR variant, which is based on Google ARCore, and still needs access to the camera to enable AR. Hence, the MAR variant also requested camera access (see Fig. 3e). Note that, despite requesting permission to use the camera, microphone, and eye tracker, no data was stored. All involved data was consumed in real-time, then discarded when the application quit (e.g., the microphone data was collected in real-time for the voice chat, but not stored at any point). Also, we chose to display a permission request for the eye tracker of the Hololens (MR), despite not using any eye-tracking functionality. Although this could be considered misleading for the participants, we maintain that this was done to gather privacy perceptions on data collection aspects, as well as measuring awareness. Therefore, we only need to pretend that eye-tracking data are collected, but do not need to collect them. The participants were given a full explanation after the study.

If the participant refused to give permission, an alert informed them that permissions were required to use the application (Fig. 3f). If they gave the requested permissions, the application connected to a self-hosted server, which enabled the multi-user experience as well as voice chat. The virtual house was then spawned on the client side (i.e., the application used by the participant), as well as the

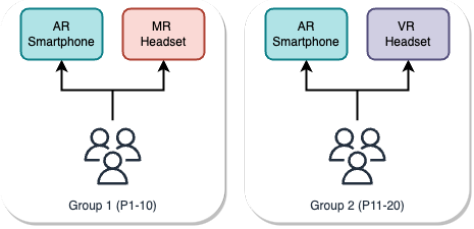


Figure 4: Each participant tried two different devices (within-subjects comparison). Participants from Group 1 tried the Hololens (MR), while participants from Group 2 tried the Quest 2 (VR) (between-subjects comparison).

avatar of the real estate agent. A second tutorial popup indicated how to open the menu to leave the virtual house or to modify the settings at any time. The tutorial also indicated how to (un)mute the microphone during the visit. From this point on, the participant was free to move within the virtual house, and could communicate with the real estate agent.

3.5 User Study Conduction

3.5.1 Participant Recruitment and Groups. The study was approved by our institution's ethical committee and data protection officer. We advertised our study in various ways, including posters, flyers, and online messages on the intranet of our institution. Before the experiment was conducted, every participant was informed about the data handling practices, and had to give explicit consent on data collection for the experiment, according to the *General Data Protection Regulation* (GDPR). Participants received a compensation of 15 euros via bank transfer.

We separated our participants into two groups of ten, as shown in Fig. 4: Group 1 tried our application with the Microsoft Hololens (MR) and the AR smartphone (MAR), and Group 2 tried the Meta Quest 2 (VR) and the AR smartphone (MAR). To eliminate potential bias from the order in which the participants tried the devices, we subdivided each group into two: one tested MAR first, and the other tested MAR last. We chose to give each participant only two variants to limit the experiment duration and the cognitive load of participants. This way, we could always compare an MR or a VR experience to an MAR experience to extend the privacy perceptions comparison to the domain of smartphones, about which users have more awareness than for other types of XR devices. Having a comparison to smartphones also allows participants to compare a traditional technology, that they use daily, to a new technology such as XR. Furthermore, MAR currently represents the biggest share of XR users, because of the high availability and compatibility of AR features in most modern smartphones [50].

3.5.2 Experiment. The organisation of the experiment is shown in Fig. 5. Each participant was greeted in person by a researcher (R1) who explained the scenario, and asked them to fill out a short questionnaire that gathered demographic data, including their age, gender identity, familiarity with XR, possession of an XR device, and *Affinity for Technology Interaction* (ATI) through an associated ATI scale [51]. R1 then supervised the experiment by indicating a first XR device to the participant, and helped them use the device (e.g., put the VR headset on). In addition, participants from Group 1 went through the native Hololens eye-tracking calibration process before launching the application. This process was automatically proposed by the Hololens upon detecting the irises from a new user. We decided to not hide this function from the participants to let them have a realistic experience with the device, as they would if they bought and used a Hololens. We do not consider this to have nudged the participants, since the calibration process was done on the OS level, and was thus entirely separated from our application. The experiment lasted ca. 30 minutes, including the time it took the participant to fill out the questionnaire, adjust the headset, and get accustomed to the device.

Once within the virtual environment, the participant would be virtually greeted by the real estate agent (R2) who would guide them through the house for the visit. R1 stayed for the experiment in the same room as the participants. R2 was in a different room, thus only meeting the participants virtually and communicating via real-time voice chat within the app.

When running the application on all XR devices, the participant was able to move freely inside the room where the experiment was conducted. We have adapted the virtual house's proportions and position to the size of the physical room. Thus, the participant's movements in the room also made them move within the virtual house. In the VR variant, participants stayed within a safe zone, as they could not see their surroundings, and moved in the house using the controllers.

3.5.3 Semi-structured Interviews. Once the participants are done with the experiment with both given XR devices, they sit with R1 for a semi-structured interview. The interviews lasted around 25 minutes on average and covered three main themes.

We first start with **permission requests** as the participant's entry point. Understanding the reasons behind their choices when being asked to give sensor access to an application has multiple advantages. First, it allows us to draw a comparison with the results of studies from a time when permission requests were not systematised in XR devices (e.g., [11]). Second, it lets us follow a logical order that matches the participant's chronological interactions with a new application.

Next, we consider subsequent **data collection** aspects. Based on the permission requests, we ask our participants their beliefs on the types of data they think are collected, and the sensitivity of said data. This first estimation about sensitivity is not meant to be precise (i.e., we simply ask whether they think the data they mentioned is sensitive data or not), because participants do not always list the same data, and more precise questions on privacy concerns over cameras, microphones and eye trackers come later in the interview. This way, we give them multiple opportunities to reflect on these topics, while ensuring we gather their perceptions more than one time, in case their opinions change during the interview. Note that we consider their answers no matter whether they are right or wrong (and do not correct them in case their guess is wrong until the end of the study), as the purpose of these questions is primarily to assess their awareness regarding data collection.

We finally consider the underlying **privacy perceptions and behaviour** on the associated devices. We begin with questions about the privacy settings of the application, the choices made by participants when encouraged to disclose personal information,

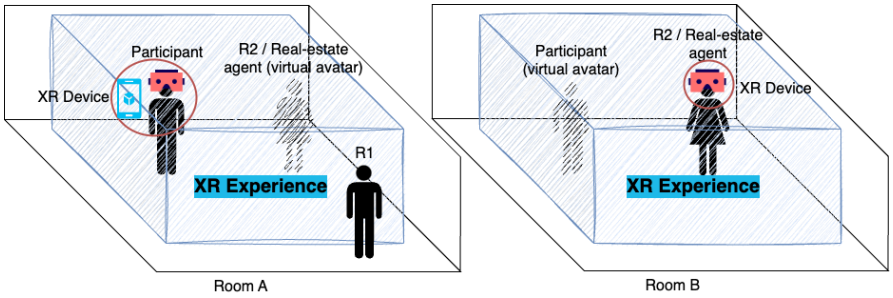


Figure 5: Overview of our experiment. Each participant was located in room A room with Researcher 1 (R1) who supervised the experiment, while Res. 2 (R2) acted as a real estate agent in a separate room B, and only interacted with the participants virtually. The participants experienced the XR app twice with a different XR device each time. R2 always used a VR headset.

and their motivations to interact with the settings. Then, we ask the participants to do a comparison of the XR experiences, first through aspects we relate to physical privacy, such as immersion and self-consciousness (i.e., physical privacy in virtual environments) [52, 53]. Finally, we go more in-depth by comparing the privacy perceptions that the participants have for each device. We also ask them to weigh their privacy concerns between each device they tried, and between XR technology as a whole versus more traditional technologies (i.e., smartphones, laptops). We provide our precise interview protocol in Appendix A.

3.6 Data Analysis

To assess our results [54], the semi-structured interviews were audio recorded and transcribed by R1, then co-coded by both R1 and R2. Both coders coded the first 10 participants on their own. As the main investigator [55], R1 first created a set of deductive codes based on some of the interview questions' expected answers, and completed it with inductive coding. R2, on the other hand, only used inductive coding. A first comparison was done on four random participants to check the closeness of each coder's codes. Then, we merged R2's codes into R1's codebook, which was more fine-grained and categorised. Both coders finished coding the remaining participants with inductive coding, using and updating the merged codebook. With our final codes, we went through a last deductive analysis on all interviews to ensure full coverage of important statements. We then calculated the *Inter Rater Agreement* (IRA) for all interviews. We provide our final codebook in Appendix B.

The initial IRA was of 54,8%. We argue that this initially low IRA is due to R1 having used more codes than R2, despite R2 often reaching an IRA of 100%—a phenomenon described in [56]. Then, both coders discussed their codes and negotiated for agreements when one coder used a code that the other did not. Eventually, the final IRA was of 95,1%. We did not reach full agreement due to occasional ambiguous statements from participants, resulting in different interpretations from the coders. Nonetheless, we consider that the ecological validity of our results holds.

In addition, due to the complexity of our codebook (185 codes)—implying a lower probability of having matching codes by chance—and the complexity of calculating Cohen's Kappa for such a large codebook [56], we decided not to use Cohen's Kappa to calculate the reliability, instead relying on the IRA (rather than the *Inter Rater Reliability* (IRR)). This fits exploratory studies such as ours [55].

We created categories from our codebook that naturally matched the order of the interviews. Hence, we obtained the three categories described in Sec. 3.5.3: **permission requests**, **data collection awareness**, and **privacy perceptions and behaviour**. To better categorise statements that were not only about privacy, we also added three additional categories: **reflection on XR experience**, which group statements on aspects about safety, ease of use, immersion, and self-consciousness; **understanding of technology**, which grouped statements that indicated the knowledge, understanding, and assumptions that the participants had about the devices; and a **miscellaneous** category which grouped interesting statements that did not fit into other categories.

Lastly, we coded privacy perceptions on data collection aspects and the XR devices themselves by using three coarse categories. When participants expressed that they had no particular concerns (e.g., *"I don't really care"*), we coded the statement as "Not or little concerned" alongside the data/device. When they expressed a degree of concern without using strong words or with impersonal formulations (e.g., *"You should be a little bit concerned about that"*), we coded the statement as "Somewhat concerned". Finally, when they expressed privacy concerns with strong, clear words and personal formulations (e.g., *"I am concerned. I know it tracks much more than I know"*), we coded the statement as "Concerned". We decided to use coarse categories for clearer categorisation of our participants' privacy perceptions, since they all used various ways of expressing their concerns.

4 Results

4.1 Participant Demographics

We recruited in total 20 participants, including students of our institution from various faculties. Their demographics are summarized in Tab. 3. Only $P_{4,9,13}$ are bachelor computer science students from our institute, who had never met R1 and did not see nor recognise R2, who sat in a closed room and acted as the real estate agent under a fake name (Hannah Schneider). We thus consider their participation as valid as other participants'. Additionally, due to regulations, full-time employees of our institution are not eligible to this compensation, as their time can be deduced from their working hours. Therefore, one participant could not be compensated, but still wanted to participate in the study. We do not expect this difference to have an impact on the results.

Table 3: Overview of our study's demographic data.

	ID	Age	Gender[1]	XR Familiarity[2]			XR Ownership	ATI
				MAR	MR	VR		
Group 1 (MAR / MR)	P_1	18-24	W	-	--	-		2,22
	P_2	18-24	M	-	--	-		4,11
	P_3	18-24	M	-	-	-	AR Smartphone	4,00
	P_4	18-24	M	+	-	+	AR Smartphone	3,44
	P_5	25-34	W	-	--	-		3,33
	P_6	18-24	M	+	-	+	AR Smartphone	3,33
	P_7	55+	W	-	--	-		3,11
	P_8	45-54	M	-	-	-		4,67
	P_9	18-24	W	+	+	-	AR Smartphone	4,78
	P_{10}	25-34	W	--	--	+		2,67
Group 2 (MAR / VR)	P_{11}	25-34	M	++	-	+	AR Smartphone	2,89
	P_{12}	18-24	W	+	+	+		1,56
	P_{13}	18-24	M	-	-	-		4,11
	P_{14}	25-34	M	+	-	+	AR Smartphone	5,00
	P_{15}	25-34	W	-	-	-		3,56
	P_{16}	18-24	W	+++	--	-		4,56
	P_{17}	25-34	W	-	--	+	AR Smartphone	3,67
	P_{18}	25-34	M	+	-	-		4,67
	P_{19}	25-34	PNTS	+	-	+	AR Smartphone	3,67
	P_{20}	18-24	W	-	--	-	AR Smartphone	3,44

[1] W: Woman, M: Man, PNTS: Prefer Not to Say.
[2] "--" indicates "I have never heard of it", "-": "I heard about it but I have never used it", "+": "I have used it several times in the last year", "++": "I use it several times a week", "+++":"I use it several times a day".

4.1.1 Familiarity with XR Devices. Participants had to self-report how familiar they were with AR, MR, and VR technologies in the questionnaire. Examples were given to describe the technologies (e.g., translating text in real-time with Google Translate through the camera mode was a given example of AR). Our participants are more familiar with the use of AR. VR is the most known term, but not the most used technology. MR is by far the least known and least used: only one participant reported having used it several times in the last year, while ten reported having heard about it but never having used it, and eight said they never heard about it. This is likely due to the confusing nature of the term "Mixed Reality" (see Sec. 2), and MR being rather marketed for the industry.

4.1.2 Possession of XR Devices. Participants also had to indicate whether they possessed any kind of XR device, from a list of popular devices, including an "other" field. We specifically asked them to only report possessing an AR-capable smartphone in case they used AR apps with it, to avoid artificially inflating the numbers, since most smartphones are AR capable nowadays. Nine participants reported having (and using) an AR capable smartphone. The rest of the sample reported not owning any kind of XR device. We observe a few discrepancies here: P_3, P_{17}, and P_{20} reported owning an AR capable smartphone, but also indicated never having used MAR (despite being asked to only report owning an AR capable smartphone if they used it actively). This suggests that these participants had a low understanding of XR technology.

4.1.3 ATI Score. Finally, participants had to fill an ATI scale [51]. The resulting affinity for technological interaction ranges from 1 to 6. We report a mean ATI score of M = 3.63 (SD = 0.89, α = .85). Nine participants have a score between 3 and 4, and seven have a score superior to 4. In comparison, recent user studies on privacy and security in VR [20, 57, 58], privacy mechanisms in ubiquitous computing [59], and bystander privacy in smart homes (i.e., other emerging and ubiquitous technologies) [60, 61, 62], report mean ATI scores between 3.83 [59] and 4.35 [20]. While slightly lower, our reported mean ATI score suggests that our participants consider themselves knowledgeable about technology, without being particularly tech-savvy.

4.2 Reactions to Permission Requests

4.2.1 No Questioning of Data Collection. All participants accepted all permission requests on all variants of the application. Only P_{13} and P_{19} initially refused both camera and microphone permissions on the MAR variant, but accepted after reading a message indicating that granting permissions was necessary to progress (see Fig. 3f).

16 participants revealed, in the interview, that the permission requests cause little to no questioning of data collection. In addition, nine said they usually give permission without thinking, and four ($P_{1,6,14-15}$) mentioned that this is especially the case for smartphone usage: *"On the smartphone, it's like, the generic pop up you get in every app, and you're just like, 'all right, okay"'* (P_6). This suggests that the habituation of users to permission request systems can lead them to lower their guard and their privacy concerns.

4.2.2 MAR Permissions Can Be Misunderstood. $P_{5,10,17,20}$ have misconceptions about the meaning of the permission choices given on the AR smartphone (see Fig. 3e). They think that "while using the app" is the more restrictive privacy choice, and understand the second choice ("Only this time") as "allow all the time". *"If I have to use my own smartphone, [...] I will allow you while using the application, not tracking all the time"* (P_{17}). In fact, choosing "Only this time" results in the permission request appearing again the next time the application is launched, making it the more restrictive choice. However, we also note that the Hololens' simpler permission system (see Fig. 3d) can be detrimental to privacy awareness. This is the case for P_5, who said the following when asked about her privacy concerns for the Hololens: *"Actually, less [than MAR] because there was this "Yes/No" question as well, at the beginning. So we were not like, "Oh, can we use the camera?" or anything"* (P_5). This suggests that the naming of the buttons as "Yes" and "No" causes less reflection from users than prompts such as "While using the app". Nevertheless, XR permission systems in their current forms fail to bring a clear understanding to all users.

4.2.3 Lack of Understanding About Need of Cameras to Track Planes in XR. $P_{4,8,13,14,17,19}$ do not understand why the MAR variant requests access to the camera. *"I could have had exactly the same experience without the camera being on. [...] But I saw that when I looked through a window, I saw the real world there. So that's what it made it augmented. But for the application that you had, it wouldn't have been necessary"* (P_8). In fact, the participants could not have had the same experience without the camera, as it would have been impossible to project the visual house around them through the AR smartphone's screen without it. In other words, these participants do not understand that the camera is used to track surfaces on which virtual content is anchored, and think the camera is only used as an optional feature. We blame this confusion on the full-scale nature of the MAR experience: the 3D model of the virtual house is scaled 1:1 with the real world, differing from traditional MAR experiences, where smaller objects are projected on a surface such as a table. This makes the frames of the camera only visible through the windows of the virtual house (see Fig. 6), which is

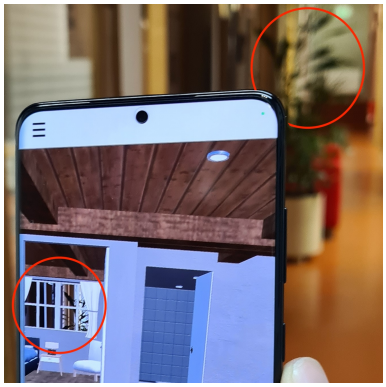


Figure 6: Full-scale projection of the virtual house (MAR). Camera frames (e.g., the plant in the background) are only visible through the virtual windows.

the only visual cue about camera activity that participants noticed, aside from the MAR permission request. No participant mentioned the green sensor usage indicator at the top right corner of the screen, despite being a feature of Android 12, which was released in 2021 [63]. This lack of understanding requires new, adapted sets of tutorials and permissions in modern OSs, such as permission to track/scan surfaces when using MAR.

4.2.4 Assumption That It Is Necessary to Grant Permissions to Use the App. $P_{1,5,7,11,17}$ assume that they must grant permissions, otherwise the app will not work, and therefore accept without even trying to refuse. This is perceived as a frustrating non-choice by P_5 and P_7: *"Well, they're [permission requests] a nuisance. I mean, if you disagree, the application will not start. So what choice do you have?"* (P_7). Despite existing recommendations for modular application design [64, 15], users can still feel like they are forced to grant permissions to use an app. Thus, developers should increasingly design their apps modularly, and clearly indicate when permissions are linked to optional features, so that refusing permissions for a given feature does not stop a user from using the app [64].

4.3 Data Collection Awareness

We now report the answers of our participants regarding what data they thought were collected by the applications, the perceived sensitivity of these data, and the reasons behind their opinions.

4.3.1 Camera Data. 11 participants indicated that camera data was collected, and 9 of them consider camera data sensitive. When discussing camera perceptions later in the interview (i.e., also with participants who did not initially guess about the use of camera data), we observed that 14 participants are concerned about XR devices recording their private environment. However, they do not develop this further, and thus show a lack of awareness on the underlying privacy risks (see Tab. 2, e.g., hand tracking [35], sensitivity of spatial data [37]).

In addition to this overall lack of awareness on XR camera data collection, eight participants are uncertain whether the cameras of the devices also film their face, and five of them specifically expressed concerns over front camera data collection ($P_{10,13,14,17,20}$). Regarding the MAR experience, P_{18} said: *"It was not stated which camera it would use, so it could use both, kind of"*. This underlines the need for more clarity regarding camera use in MAR experiences, which could be given with, e.g., more specific frontal and back camera permission requests.

4.3.2 Microphone Data. 18 participants could identify microphone data. 14 of them could immediately tell that this data is collected so that they can communicate with the real estate agent with the voice chat, which may explain why the awareness on microphone data collection is much higher than on camera data. Participants who guessed about microphone data collection are split about sensitivity, as nine of them consider it sensitive. $P_{3,4,8,10,18,19}$ are aware about the possibility of voice tampering. This is likely due to the recent availability and popularity of Artificial Intelligence voice imitation models to the public. One way to protect the users' voice, while letting them enjoy voice chats in XR experiences, lies in voice modulators, as encouraged in [12].

4.3.3 Eye-Tracking Data. 10 participants indicated that eye tracker data was collected (nine from Group 1, and one from Group 2). Interestingly, P_{15}, from Group 2, also thought that eye-tracking data was collected by the VR headset, despite the Quest 2 not having eye trackers and the absence of eye-tracking permissions in the VR variant (see Tab. 2). In Group 1, $P_{4,8,10}$ consider eye-tracking data sensitive, while P_2 and P_6 consider it not sensitive. The remaining four of Group 1 who guessed about the use of eye-tracking data in the application ($P_{3,5,7,9}$) did not initially comment about its sensitivity, or commented about the general sensitivity of XR data. $P_{3,4,7,8}$ are aware that eye-tracking can reveal their interests and be used for, e.g., biometric advertising (see Tab. 2). *"In any application, I would be very aware, like when I'm on Instagram or something, when they see on which picture I look. That would be a jackpot for [...] advertising when they know where I look exactly."* (P_4). While these results on eye-tracking data collection awareness are encouraging, only our more privacy-aware participants knew about its sensitivity. Therefore, this knowledge also needs to be given to less privacy-aware users.

4.3.4 Movement Data. 11 participants indicated that data regarding their movements was collected. However, only P_{13} and P_{18} consider movement data to be sensitive, and only P_{18} is aware that analysis on movement data could reveal information about them. We argue that findings on movement data sensitivity (e.g., [27, 28]) have not yet reached the general population. This concurs with the insights of XR experts seen in [15]. In contrast to eye-tracking data, about which participants from Group 1 are more cautious, the major lack of awareness that we observe on movement data sensitivity is striking. Work in informing—and protecting—users about these data is essential for the future of XR.

4.3.5 Other Types of Data. Participants also indicated other types of data that were never used by our application. These include GPS location ($P_{3,11,17}$), inferred demographic data (e.g., size, age, gender) ($P_{5,13}$), and IP address (P_{17}). This suggests that participants may expect data to be collected without their informed consent. For example, participants who thought that the GPS location was used did not get an associated permission request, although access to the device's precise GPS location requires permission on Android (the Hololens and Quest 2 do not have GPS, as shown in Tab. 2). In addition, P_{12} and P_{14} thought that the position and rotation of

the device were used. Although this is technically true, these data are in fact only used internally by the device for the XR technology to function, and not directly by our application. This shows that participants do not always assume that a permission request is mandatory for data to be collected—which is true, since accelerometer and gyroscope data usage does not require permissions. In other words, it is hard for users to know what data can or cannot be obtained without their consent. This challenge is made all the more difficult to solve by the difference in permission systems from the various OSs present in XR devices. For example, access to the camera feed requires permission from the user on Android (MAR), but not on the Hololens (MR) nor the Quest (VR). Despite this difficulty, efforts in unifying XR permission systems are required for more transparency toward end-users regarding data collection.

4.4 XR Privacy Perceptions and Behaviour

4.4.1 Privacy Perceptions. We provide an overview of our participants' privacy perceptions on the tested XR devices in Tab. 4, and their privacy perceptions on sensor data collection in Tab. 5.

Participants are in general concerned about MAR which is seen as an extension of smartphone usage. In total, 15 participants are somewhat concerned or concerned about their privacy with MAR (see Tab. 4). These concerns are linked to camera data collection, as 13 of them (16 in total) are also somewhat concerned or concerned by cameras in MAR (see Tab. 5). We argue that these concerns are due to the aforementioned awareness that they have regarding camera data collection. Furthermore, MAR concerns seem to stem from smartphone concerns, as participants tended to answer MAR-related questions with regular smartphone usage examples. *"I feel like it's just the same as when I'm using FaceTime or my camera app. So there's no difference"* (P_{12}). $P_{8,11-12,14-15}$ did not see a difference between a MAR app and a normal smartphone app. In addition, $P_{7,19-20}$ revealed that they specifically have concerns about smartphones because they have more knowledge about them: *"I would always be a bit more [...] conscious with the phone because I am more accustomed to use a phone and [...] I have more knowledge about it."* (P_{19}). We therefore theorize that MAR privacy concerns are inherited from smartphone privacy concerns.

MR gathered the most mixed concerns. Privacy concerns over MR are slightly more distributed between not and somewhat concerned (see Tab. 4). Still, the Hololens got two "concerned" reactions from P_4 and P_7. Concerns about the Hololens are directly linked to camera data collection and eye-tracking (and its potential for biometric advertising), as seen in Tab. 5. $P_{1,5,10}$ in Group 1, who are unconcerned about eye-tracking, could not tell what could be done with such data: *"This eye-tracking [...], it's so special. It's very personal and so special. But I don't know what someone would use this for"* (P_{10}). Given that incomplete information is a source of privacy uncertainty [52], we attribute the lack of awareness of these participants on eye-tracking data to the lack of technological knowledge on these sensors, which are still recent additions on XR devices. Consequently, further efforts should be made to raise the already good awareness on eye-tracking data sensitivity.

VR gathered the least amount of concern. In Group 2, $P_{11,12,14-16,19}$ feel little or no concern about VR, and $P_{11-12,14-16,19-20}$ have low awareness and concerns about the use of cameras in VR, as seen in Tab. 5. One reason for this—aside from the lower acceptance rate and, thus, lower knowledge about it—is that immersion can distract from privacy concerns. $P_{6-8,11,17,20}$ mentioned that the feeling of immersion and entertainment given by VR (or MR) lowers their privacy awareness: *"It [VR] provides me with a more immersive experience. So I kind of forget where I am... And all the things I see, it's all virtual, like the landscape outside the window [...] So I don't really think about the private things when I'm using it."* (P_{11}). Therefore, the factor of immersion on privacy concerns should be considered in future XR PETs. Another factor lowering VR concerns might be the perception of VR headsets as devices only meant for one use case (e.g., gaming) that hold less personal data than, e.g., a smartphone, as $P_{12,17,18}$ revealed. *"I think normally I would use VR for having fun and not for, like, shopping or social life"*. (P_{18}).

Table 4: Privacy perceptions of both groups for each device.

Group	Level of concern	AR Smart	Hololens	Quest 2	XR (General)
Group 1 (P_{1-10})	Not/little concerned	4	4	N/A	4
	Somewhat concerned	5	4	N/A	3
	Concerned	1	2	N/A	3
Group 2 (P_{11-20})	Not/little concerned	1	N/A	6	6
	Somewhat concerned	9	N/A	3	3
	Concerned	0	N/A	1	1

Table 5: Privacy perceptions of our participants on sensor data collection for each XR device. 20 participants tried MAR, whereas 10 tried MR and 10 tried VR.

Sensor	Level of concern	AR Smart.	Hololens	Quest 2
Camera	Not/little concerned	4	2	7
	Somewhat concerned	15	8	2
	Concerned	1	0	1
	Σ	20	10	10
Mic.	Not/little concerned	13	5	7
	Somewhat concerned	7	5	2
	Concerned	0	0	1
	Σ	20	10	10
Eye-tr.	Not/little concerned	N/A	3	N/A
	Somewhat concerned	N/A	6	N/A
	Concerned	N/A	1	N/A
	Σ	0	10	0

Comparison of XR Privacy Perceptions. In Group 1, P_{10} considers that MAR is more concerning than MR. $P_{1,8,9}$ consider that MAR is as concerning. The remaining six consider MAR as less concerning (P_{2-7}). In Group 2, eight participants consider MAR as more concerning than VR ($P_{11,12,14,16-20}$). P_{15} considers MAR as concerning, and P_{13} considers MAR as less concerning. In other words, when comparing MAR to MR, MR is considered more or as concerning by nine participants of Group 1, despite similar concerns for both technologies (see Tab. 4). However, when comparing MAR to VR, MAR is considered at least as concerning or more than VR by eight participants of Group 2. A possible explanation for this stark contrast could be that participants have different perceptions of a given device (e.g., MAR) depending on what they compare it to. Following this, concerns on MAR may be higher in Group 2

because it was compared to VR, which gathered the least concerns. These results should be confirmed in further studies to exclude possible effect sizes.

Comparison of XR Against Smartphones and Computers. 10 participants consider that XR is more concerning than traditional technologies, such as smartphones and computers. Of these participants, $P_{5,15}$ are nonetheless not or little concerned by XR technologies in general, $P_{2,6,9,17}$ are somewhat concerned by XR, and $P_{3,4,7,13}$ stated that they feel very concerned by XR technologies in general. Different reasons behind these perceptions were given, including the fact that XR devices can capture the user's head and/or eyes ($P_{2,15}$), scan their surroundings ($P_{3,9}$), collect much more data (P_4), or simply because they do not know about the technology (P_5). The more concerned participants mentioned various topics related to privacy invasion, such as biometric advertising (P_4) and mass surveillance (P_7). When asked how concerned she feels about her privacy regarding XR technologies, P_7 said: *"Very much. I mean, I'm not so much concerned about myself, but I'm concerned about your generation and everyone following. [...] Some people think they have nothing to hide. That's not true. That's just because they are not tracked. [...] In China, everything is tracked. And you know, you get your score and... We're not far from that. And we all have something to hide."* (P_7). The invasive character of XR perceived by these participants may be shared by a larger share of the population, posing a challenge to the full adoption of these technologies. On the other hand, we observe a considerable, yet varying degree of awareness regarding the sensitivity of XR data. More work is needed to make the sensitivity of XR data more transparent to unaware users, and better protect their privacy to foster the adoption from more privacy-aware individuals.

$P_{10,11,14,20}$ consider that XR is less concerning than traditional technologies. The most given reason was that XR implies less sensitive data and operations: *"It's much more sensitive what I'm doing when I'm browsing [with a laptop]. [...] Online banking or something, I won't do in VR."* (P_{14}). This relates to the aforementioned assumption (which was also shared by these participants) that XR headsets are mainly meant for one use case (e.g., gaming). These participants do not perceive HMD-based XR devices as versatile as, e.g., smartphones. They cannot imagine having as much personal data on XR devices as they have on their phone, and therefore feel less concerned about the headsets. Although such use cases may not yet be realistic today, they should nonetheless already be considered by researchers, vendors, and developers, when creating XR PETs.

The remaining $P_{1,8,12,16,18,19}$ consider that XR is as concerning as traditional technologies. $P_{1,8,12,16}$ also do not feel concerned about XR, while P_{18} and P_{19} feel somewhat concerned. Here, participants weigh the sensitivity of their data similarly, despite considering that different data are involved. *"I think they collect different data. But they are kind of similar in how private it is. [...] I think they all can collect data and, it's not worse than with laptops or smartphones."* (P_{18}). Although acknowledging that different data are at stake is already commendable, raising awareness is necessary for the share of users who, like these participants, do not perceive XR data (especially biometric data) as particularly more sensitive than more common personal data. This awareness is necessary for those users to make informed privacy decisions.

4.4.2 Participants' Behaviour. We here describe privacy-related actions done by our participants during the experiment.

Interaction with Settings. All participants opened the settings during the experiment. When using the application the second time, $P_{2,4,7,9,18}$ opened the settings page before joining the virtual tour, by anticipation (since they were encouraged to do so with the first device, as described in Sec. 3.2). No participant verified the other setting about the state of muting when joining the virtual room. We asked them if they saw or read the setting or not, when visiting the room. 10 did read it, and the rest did not or could not remember what it was. 14 participants who did not read it said that they were concentrated on the current task (i.e., showing their name). Interestingly, P_{13} and P_{18} also mentioned that they did not pay attention to this setting because its checkbox was unchecked by default: *"If I spotted one that was turned on by default, I would have looked at that. [...] If it was already off, then it didn't bother me"* (P_{13}). This underlines the importance of opt-in and privacy by default mechanisms in applications [65].

Impacting Factors on Virtual Behaviour. 12 participants agreed to disclose their full name because they sought equal to equal communication, as they knew the real estate agent's name—Hannah Schneider—but she did not. When asked about her motivations to show her full name publicly, P_{10} said: *"The moment she mentioned it, I was like, 'Oh my god, how impolite that I see her name and she [doesn't] see my name!'. And [I agreed] so that we are more in an even communication situation"* (P_{10}). In addition, six participants showed signs that their behaviour was partly inherited from real-life social customs: *"Even if I knew this was a virtual person there, I always had the same, you know, [reflex of] standing away from a person [...] I am not going [to] ever touch her or go into her personal space"* (P_{10}). Furthermore, 11 participants indicated a lowered feeling of body perception when using the MR or VR device, which relates to the fact that all 20 participants declared having had a more immersive experience with these devices. Given the mention of physical privacy and real-life social customs, more research is needed to determine the extent to which lowered body perception in immersive XR experiences impacts the virtual behaviour and privacy perceptions of users.

5 Discussion

5.1 XR Privacy Concerns

5.1.1 Concerns Over XR Devices. We answer **RQ1** with the finding that participants are more concerned about MAR and MR than VR. While more participants tried MAR than MR in total, concerns over MAR and MR score similarly in the first group. P_4 and P_7 feel especially concerned about the Hololens, and P_7 feels especially concerned for MAR (see Tab. 4). Possible reasons for the concerns over MR include the subsequent concerns over eye-tracking (seven participants of Group 1), cameras (eight of Group 1), and the overall novel/unknown character of the device. This relates to the results of Gallardo et al. presented in [19], where 13 out of 21 participants were uncomfortable or conflicted with eye-tracking and/or video data collection. However, VR does not spark as many concerns. Participants from Group 2 feel more relaxed when comparing the use of a VR headset to the use of a smartphone, as they do not imagine having as much personal and/or sensitive data (e.g., banking

data) on a VR device. Similarly, VR is sometimes considered as a technology mostly or only made for gaming, and the immersion it provides can distract users from privacy concerns. The perceived entertaining nature of the technology has also been observed in [20], and may be a reason for the observed difference in concerns over the other variants. As such, care should be given to mitigate the distracting factors of entertainment and immersion on VR privacy perceptions. We also recommend further quantitative studies with bigger sample sizes to support these results.

5.1.2 Impacting Factors on Privacy Concerns. In addition, we noted factors that impacted the privacy concerns of participants regarding XR. In the following, we discuss these factors and compare them to other works on privacy perceptions in other new technologies.

Concerns Depend on Knowledge of Technology. Participants often expressed not being knowledgeable about XR (observed for 13 participants). Lack of knowledge is a known source of privacy uncertainty, as shown in [52]. The current low user acceptance of AR/MR and VR HMDs compared to smartphones, and thus the different amount of knowledge among XR technologies, partly explains the observed difference in privacy perceptions. These results align with the insights of XR experts relayed in [15], stating that users do not understand why their data is needed; and with works on privacy perceptions on other new technologies, such as smart speakers [66] and smartwatches [67]. Consequently, more transparency must be given to users about XR data collection, and about the sensitivity of these data (e.g., body movement data), as encouraged by [12, 15, 13, 21].

Concerns Depend of Involved Companies. $P_{3-4,8,12,13}$ mentioned their mistrust of brands, such as Google or Meta. Three of them (five in total) also mentioned a lack of transparency regarding data collection from these companies. Concerns over companies were also expressed by VR users and developers in [11], as well as for smart speakers [66] and smartwatches [67]. Companies must provide more transparency to users regarding data collection and the purpose of this collection, to increase user acceptance and use intention, as observed by [13].

Concerns Depend on Presence of Bystanders. Four participants expressed concerns over the presence of bystanders—physical bystanders outside of the XR experience, but also virtual bystanders within multi-user experiences. The reasons behind these concerns included ethical issues of filming others in public spaces (P_8), the potential for virtual bystanders to eavesdrop in multi-user experiences (P_{13}), and the impossibility of seeing what others do when using VR ($P_{18,20}$). We find that these concerns are exclusive to XR technologies and observed in other user studies [8, 9, 10, 17, 18]. The next generations of XR devices will need to implement PETs to protect the privacy of bystanders (e.g., [43]).

5.2 XR Data Collection Awareness

We answer **RQ2** by suggesting that participants have relatively low awareness regarding camera data and biometric data collection, such as body movements. Overall, the permission requests shown on XR devices—a feature requested by VR developers in the past [11]—do not contribute to increased data collection awareness. We observe that participants often show no questioning of data collection when confronted with permission requests, especially with MAR. The given choices are sometimes misunderstood, and we note occasional frustration due to the impression of having no choice but to accept the requests. These observations are similar to the findings reported in [68], underlying the still limited benefits of permission request systems on user awareness.

When comparing awareness on the type of data, we see that participants are less aware about the collection of camera data than microphone and eye tracker data. This gap in identifying the types of collected data may be caused by multiple factors. First, only the MAR variant has a camera permission request (see Sec. 3.4.2), but all variants have a microphone permission. Second, the eye-tracking permission was new to all participants of Group 1 (who tried the Hololens), which may have left a bigger impression than the more usual camera permission. Lastly, the collection of microphone data makes sense to participants because they can easily map this data to the voice chat functionality. In other words, a concrete action is performed with the collected data, which may help realise that this data is collected. This is not the case with camera data, which are only used for the XR technology to function, leading back to the lack of understanding about camera usage in XR (see Sec. 4.2.3).

Therefore, a way to raise user awareness regarding camera use in XR lies in better explaining the underlying plane tracking mechanism. This could be done with new XR-specific permissions in modern OSs, especially Android and iOS which share the widest user base of XR users. For XR devices that always require cameras to function, a comprehensive tutorial could be given to users when using the device for the first time, rather than adding a superficial camera permission that would be mandatory to give anyway. Showing that cameras are necessary for the functioning of XR technology, through transparent information about data collection purposes, is critical for lay users to give informed consent when using XR apps that require sensor access, as discussed in [14]. It is however important not to lower users' concerns with justifications about camera usage just to convince them to accept permission requests. Importantly, further camera usage should be clearly separated from this core functional requirement for more transparency. This separation is especially crucial for future XR devices that may require a constant camera and microphone access, as foreseen in [17]. These additional usage purposes (e.g., face recognition) should also be subject to specific permission requests [14].

5.3 Limitations

We acknowledge certain limitations in our study, which we categorize as limitations related to our sample demographics, and limitations regarding methodological aspects.

5.3.1 Sample Demographics. We first acknowledge that our sample is partly composed of non-XR users, which could limit the generalisability of our findings regarding the behaviour of actual users. However, we conducted this study in a context where XR remains emergent, and where non-users represent the majority of the population, thus being more representative. On the other hand, daily users could also reflect a more relaxed privacy attitude towards the tested devices. For these reasons, we chose to accept participants with any level of knowledge and familiarity about XR in our study.

Secondly, although our sample was balanced between genders, most participants were students, and 16 of them were under 35 years

old. Given that privacy perceptions and awareness are known to differ depending on the age of individuals [69, 70], the concentration of younger participants in our sample may have resulted in missing out on more privacy-aware standpoints from older individuals. Still, the students in our sample belong to the 18-24 and 25-34 years old categories, which represent the biggest share of individuals interested in AR and VR (and thus, may be more willing to adopt XR) in the U.S. in 2022 [71, 72].

Lastly, we note that two participants, respectively from the 45-54 years old and 55+ year old categories, are both in Group 1 rather than being distributed in both groups. This was because participants were assigned to groups based on their availability due to our study setup. Still, we observed that both had different privacy perceptions for the same devices. We also went against adding new participants later on, as their privacy perceptions could be influenced by factors to which our initial participants were not exposed.

5.3.2 Methodological Aspects. We do not provide a quantitative analysis of our results, because of the small sample in our study (n=20). However, for an exploratory study in the context of new technologies that are emerging, we primarily aim to observe and understand the opinion of individuals on devices they are mostly experiencing for the first time. Given the range of acceptable sample sizes in the field of usable privacy [40] (see Tab. 1), we settled for a sample of 20 participants, whom we interviewed in depth after having them experience a concrete XR application.

Furthermore, 14 participants revealed that the context of the study—being done in a lab, and not with their own devices—lowered their privacy concerns, which is a known limitation of lab studies. Despite this, participants could imagine situations where they would use their own devices in a more personal setting (e.g., at home), and indicate their concerns on these suppositions. We coded their answers based on these insights as well. For example, when asked about his concerns over the camera usage for MAR, P_2 said: *"I don't know if it really concerns my privacy, because it wasn't my house. But if it was my house, I think it would be a little bit problematic, because others could save the information."*. Based on this, we considered P_2 to be somewhat concerned by the use of cameras in MAR. Still, in light of the difference in concerns of participants in the context of the lab study, we suggest that future work in the area should attempt to observe users in a more personal context.

Among those 14 participants, $P_{2,10,12,15,18}$ said that the context of the study made them accept the permissions. P_{15} and P_{18} still mentioned that they would have given more attention to the permission requests in a real-life context. On the other hand, nine participants said they did not think about privacy aspects during the experiments, nine said they almost did not (e.g., only thought slightly about giving permissions), and P_9 and P_{17} said they thought a bit about them. This shows that while the context of the study might have lowered the privacy concerns of the participants, we did not prime them with an obvious privacy task.

Lastly, we acknowledge the limitation of not having a group directly comparing MR and VR perceptions, which may have added interesting insights. Still, we perceive benefits in lowering the cognitive load of our participants by only comparing two XR devices instead of three: Repeating the same tasks three times may have lowered their attention regarding the respective experiences and introduced confusion between their perceptions of the different technologies. We also still take advantage of the mixed method nature of our design, and compare the privacy perceptions of P_{1-10} on MR against the privacy perceptions of P_{11-20} on VR through the relative perception of MAR common to both groups.

6 Conclusion and Future Work

XR is set to be the backbone of the Metaverse, expanding the potential for interconnected experiences across different devices and realities. However, the research community lacks knowledge about how users perceive these new experiences, and has until now rather focused on each technology individually. We argue that a global vision is required to be able to assist XR users with state-of-the-art PETs in the coming era. Therefore, to understand the privacy perceptions of users on global XR, we conducted a qualitative lab study on XR privacy perception comparisons (n=20). Our participants are more concerned about MAR and MR than VR. Our results also suggest that the social behaviour of individuals in virtual worlds is partly inherited from real-life social customs (e.g., respecting someone's private sphere by distancing). In light of the results of our exploratory study, future research directions can be considered. We make propositions on both XR privacy awareness and on the virtual behaviour of users.

Raising XR Data Collection Awareness. For MAR, work on camera permission requests is required to clarify the type of camera used by applications. Alternatively, new sets of permissions specifically designed for XR contexts are possible. For MR, efforts from the industry and the research community are needed to dissipate the confusing nature of the term, and adopt one naming convention for MR devices. This, along with more work on raising awareness on eye-tracking, should help users understand the technology and associated privacy risks better. For VR, the given image of a gaming-only device may distract users from privacy risks. Thus, work is needed to raise awareness about privacy risks, especially about movement data. This can be done by designing new PETs that give information about privacy risks to users, and/or give them more control over sensor data collection. In addition, to further understand the influencing factors of individuals' privacy perceptions, future studies may observe whether there are behavioural differences between users depending on the systems they use on a daily basis (e.g., Android, iOS, Windows, Linux, macOS). Lastly, we encourage XR developers to clearly indicate the purpose for which they use data in user-readable forms, in particular about camera data. This could be done by adding a short explanation about how camera data is used to calculate surfaces to project virtual content.

Understanding User Privacy Perceptions and Behaviours in Different XR Virtual Social Contexts. The inequality in immersion and difference of environments from one XR variant to another will create challenges that will need to be addressed. This includes protecting users in more immersive settings (i.e., MR and VR users) from, e.g., virtual sexual harassment, and preventing the privacy of bystanders from being compromised. In general, guidelines and standards are needed for developers of cross-platform XR social experiences, so that end-users may enjoy each variant safely.

Acknowledgments

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Google. 2022. Google Play Services for AR. (2022). Retrieved Sept. 2022 from play.google.com/store/apps/details?id=com.google.ar.core.

[2] Paul Milgram, Haruo Takemura, Akira Utsumi, and Fumio Kishino. 1995. Augmented Reality: A Class of Displays on the Reality-Virtuality Continuum. In *Proceedings on Telemanipulator and Telepresence Technologies*. Vol. 2351, 282–292.

[3] Richard Skarbez, Missie Smith, and Mary C Whitton. 2021. Revisiting Milgram and Kishino's Reality-Virtuality Continuum. *Frontiers in Virtual Reality*, 2.

[4] Sebeom Park, Shokhrukh Bokijonov, and Yosoon Choi. 2021. Review of Microsoft Hololens Applications over the Past Five Years. *Applied sciences*, 11, 16, 7259.

[5] AR Insider. 2021. Virtual Reality (VR) Headset Unit Sales Worldwide from 2019 to 2024. (2021). Retrieved Apr. 2023 from www.statista.com/statistics/677096.

[6] Stylianos Mystakidis. 2022. Metaverse. *Encyclopedia*, 2, 1, 486–497.

[7] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Computing Surveys (CSUR)*, 52, 6, 1–37.

[8] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies. In *Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems (CHI)*, 2377–2386.

[9] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (S&P)*, 392–408.

[10] Philipp A Rauschnabel, Jun He, and Young K Ro. 2018. Antecedents to the Adoption of Augmented Reality Smart Glasses: A Closer Look at Privacy Risks. *Journal of Business Research*, 92, 374–384.

[11] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Proceedings of the 2018 USENIX Symposium on Usable Privacy and Security (SOUPS)*, 427–442.

[12] Divine Maloney, Samaneh Zamanifard, and Guo Freeman. 2020. Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. In *Proceedings of the 2020 ACM Symposium on Virtual Reality Software and Technology (VRST)*, 1–9.

[13] Kirsten Cowan, Ana Javornik, and Peilin Jiang. 2021. Privacy Concerns When using Augmented Reality Face Filters? Explaining why and when use avoidance occurs. *Psychology & Marketing*, 38, 10, 1799–1813.

[14] David Harborth and Sebastian Pape. 2021. Investigating Privacy Concerns Related to Mobile Augmented Reality Apps–A vignette Based Online Experiment. *Computers in Human Behavior*, 122, 106833.

[15] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In *Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI)*, 1–12.

[16] Philipp Sykownik, Divine Maloney, Guo Freeman, and Maic Masuch. 2022. Something Personal from the Metaverse: Goals, Topics, and Contextual Factors of Self-Disclosure in Commercial Social VR. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI)*, 1–17.

[17] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2022. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 6, 4, 1–35.

[18] Joseph O'Hagan, Julie R Williamson, Florian Mathis, Mohamed Khamis, and Mark McGill. 2023. Re-evaluating VR User Awareness Needs During Bystander Interactions. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI)*, 1–17.

[19] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative Privacy Concerns About AR Glasses Data Collection. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, 2023, 4, 416–435.

[20] Jingjie Li, Sunpreet Singh Arora, Kassem Fawaz, Younghyun Kim, Can Liu, Sebastian Meiser, Mohsen Minaei, Maliheh Shirvanian, and Kim Wagner. 2023. How Interactions Influence Users' Security Perception of Virtual Reality Authentication? arXiv:2303.11575.

[21] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI)*, 1–24.

[22] Chris Warin and Delphine Reinhardt. 2022. Vision: Usable Privacy for XR in the Era of the Metaverse. In *Proceedings of the 2022 European Symposium on Usable Security (EuroUSEC)*, 111–116.

[23] Brendan David-John, Kevin Butler, and Eakta Jain. 2022. For your Eyes Only: Privacy-Preserving Eye-Tracking Datasets. In *Proceedings of the 2022 ACM Symposium on Eye Tracking Research & Applications (ETRA)*, 1–6.

[24] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. 2019. Privaceye: Privacy-Preserving Head-Mounted Eye Tracking using Egocentric Scene Image and Eye Movement Features. In *Proceedings of the 2019 ACM Symposium on Eye Tracking Research & Applications (ETRA)*, 1–10.

[25] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-Aware Eye Tracking using Differential Privacy. In *Proceedings of the 2019 ACM Symposium on Eye Tracking Research & Applications (ETRA)*, 1–9.

[26] Brendan David-John, Kevin Butler, and Eakta Jain. 2023. Privacy-Preserving Datasets of Eye-Tracking Samples with Applications in XR. *IEEE Transactions on Visualization and Computer Graphics*, 29, 5, 2774–2784.

[27] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding User Identification in Virtual Reality through Behavioral Biometrics and the Effect of Body Normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI)*.

[28] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal Identifiability of User Tracking Data during Observation of 360-degree VR Video. *Scientific Reports*, 10, 1, 17404.

[29] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James O'Brien, Louis Rosenberg, and Dawn Song. 2023. Unique Identification of 50,000 Virtual Reality Users from Head & Hand Motion Data. In *Proceedings of the 2023 USENIX Security Symposium (USENIX Security)*.

[30] Vivek Nair et al. 2023. Inferring Private Personal Attributes of Virtual Reality Users from Head and Hand Motion Data. arXiv:2305.19198.

[31] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI)*, 1–12.

[32] Ismat Jarin, Yu Duan, Rahmadi Trimananda, Hao Cui, Salma Elmalaki, and Athina Markopoulou. 2023. BehaVR: User Identification Based on VR Sensor Data. arXiv:2308.07304.

[33] Pier Paolo Tricomi, Federica Nenna, Luca Pajola, Mauro Conti, and Luciano Gamberini. 2023. You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality. *IEEE Access*, 11, 9859–9875.

[34] Carter Slocum, Yicheng Zhang, Nael Abu-Ghazaleh, and Jiasi Chen. 2023. Going through the Motions: AR/VR Keylogging from User Head Motions. In *Proceedings of the 2023 USENIX Security Symposium (USENIX Security)*, 159–174.

[35] Jonathan Liebers, Sascha Brockel, Uwe Gruenefeld, and Stefan Schneegass. 2022. Identifying Users by Their Hand Tracking Data in Augmented and Virtual Reality. *International Journal of Human–Computer Interaction*, 40, 2, 409–424.

[36] Jaybie Agullo De Guzman, Aruna Seneviratne, and Kanchana Thilakarathna. 2021. Unravelling Spatial Privacy Risks of Mobile Mixed reality Data. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 5, 1, 1–26.

[37] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. A First Look into Privacy Leakage in 3D Mixed Reality Data. In *Proceedings of the 2019 European Symposium on Research in Computer Security (ESORICS)*, 149–169.

[38] Brent Insko and Lisa Watts. 2022. Cross-Platform XR Development Using Open Standards: An OpenXR Tutorial & Use Case. Augmented World Expo. https://www.youtube.com/watch?v=ctXGa-4SXZA.

[39] Stefanie Pötzsch. 2009. Privacy Awareness: A Means to Solve the Privacy Paradox? In *Proceedings of the 2008 IFIP Summer School on the Future of Identity in the Information Society (FIDIS)*. Springer, 226–236.

[40] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2022. Prototyping Usable Privacy and Security Systems: Insights from Experts. *International Journal of Human–Computer Interaction*, 38, 5, 468–490.

[41] Sarah M. Lehman, Abrar S. Alrumayh, Kunal Kolhe, Haibin Ling, and Chiu C. Tan. 2022. Hidden in Plain Sight: Exploring Privacy Risks of Mobile Augmented Reality Applications. *ACM Transactions on Privacy and Security*, 25, 4, 1–35.

[42] Alessandro Acquisti, Ralph Gross, and Fred Stutzman. 2014. Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, 6, 2.

[43] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y Charlie Hu, and Bo Ji. 2023. BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems. In *Proceedings of the 2023 Annual International Conference on Mobile Systems, Applications and Services (MobiSys)*, 370–382.

[44] Elmira Deldari, Diana Freed, Julio Poveda, and Yaxing Yao. 2023. An Investigation of Teenager Experiences in Social Virtual Reality from Teenagers',

Parents', and Bystanders' Perspectives. In *Proceedings of the 2023 Symposium on Usable Privacy and Security (SOUPS)*, 1–17.
[45] Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. 2022. Shoulder-Surfing Resistant Authentication for Augmented Reality. In *Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI)*, 1–13.
[46] Tobias Lange, Philipp Matheis, Reyhan Duzgun, Melanie Volkamer, and Peter Mayer. 2024. Vision: Towards Fully Shoulder-Surfing Resistant and Usable Authentication for Virtual Reality. In *Proceedings of the 2024 Symposium on Usable Security and Privacy (USEC)*.
[47] Sarah M. Lehman, Abrar S. Alrumayh, Haibin Ling, and Chiu C. Tan. 2020. Stealthy Privacy Attacks Against Mobile AR Apps. In *Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS)*, 1–5.
[48] David Harborth, Majid Hatamian, Welderufael B. Tesfay, and Kai Rannenberg. 2019. A Two-pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality Applications. In *Proceedings of the 2019 Hawaii International Conference on System Sciences (HICSS)*.
[49] Khronos. 2022. OpenXR Overview - The Khronos Group Inc. (2022). Retrieved Sept. 2022 from www.khronos.org/OpenXR/.
[50] eMarketer. 2021. Number of Virtual Reality (VR) and Augmented Reality (AR) Users in the United States from 2017 to 2023. (2021). Retrieved Feb. 2024 from www.emarketer.com/content/us-virtual-augmented-reality-users-2021.
[51] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) scale. *International Journal of Human–Computer Interaction*, 35, 6, 456–467.
[52] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science*, 347, 6221, 509–514.
[53] NA Moreham. 2014. Beyond Information: Physical Privacy in English Law. *The Cambridge Law Journal*, 73, 2, 350–377.
[54] Loraine Busetto, Wolfgang Wick, and Christoph Gumbinger. 2020. How to Use and Assess Qualitative Research Methods. *Neurological Research and Practice*, 2, 1–10.
[55] John L Campbell, Charles Quincy, Jordan Osserman, and Ove K Pedersen. 2013. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research*, 42, 3, 294–320.
[56] Anne Marguerite McAlister, Dennis M Lee, Katherine M Ehlert, Rachel Louis Kajfez, Courtney June Faber, and Marian S Kennedy. 2017. Qualitative Coding: An Approach to Assess Inter-rater Reliability. In *Proceedings of the 2017 ASEE Annual Conference & Exposition*.
[57] Shady Mansour, Pascal Knierim, Joseph O'Hagan, Florian Alt, and Florian Mathis. 2023. BANS: Evaluation of Bystander Awareness Notification Systems for Productivity in VR. In *Proceedings of the 2023 Symposium on Usable Security (USEC)*, 1–19.
[58] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2022. Can I borrow your ATM? Using Virtual Reality for (Simulated) In Situ Authentication Research. In *Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, 301–310.
[59] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI)*, 1–23.
[60] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction*, 6, MHCI, 1–21.
[61] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 2020 International Conference on Mobile and Ubiquitous Multimedia (MUM)*, 83–95.
[62] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *Proceedings of the 2021 International Conference on Mobile and Ubiquitous Multimedia (MUM)*, 108–122.
[63] Android. 2023. Check if Your Android Camera or Microphone is On or Off. (2023). Retrieved Oct. 2023 from support.google.com/android/answer/13532937.
[64] Kenan Degirmenci. 2020. Mobile Users' Information Privacy Concerns and the Role of App Permission Requests. *International Journal of Information Management*, 50, 261–272.
[65] Ann Cavoukian. 2009. Privacy by Design.
[66] Christoph Lutz and Gemma Newlands. 2021. Privacy and Smart Speakers: A Multi-Dimensional Approach. *The Information Society*, 37, 3, 147–162.
[67] Emmanuel Sebastian Udoh and Abdulwahab Alkharashi. 2016. Privacy Risk Awareness and the Behavior of Smartwatch Users: A Case Study of Indiana University Students. In *Proceedings of the 2016 Future Technologies Conference (FTC)*, 926–931.
[68] Kevin Benton, L Jean Camp, and Vaibhav Garg. 2013. Studying the Effectiveness of Android Application Permissions Requests. In *Proceedings of the 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 291–296.
[69] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online Privacy Perceptions of Older Adults. In *Proceedings of the 2017 International Conference on Human Aspects of IT for the Aged Population (ITAP)*, 181–200.
[70] Stan Kurkovsky and Ewa Syta. 2010. Digital Natives and Mobile Phones: A Survey of Practices and Attitudes About Privacy and Security. In *Proceedings of the 2010 IEEE International Symposium on Technology and Society (ISTAS)*, 441–449.
[71] Vorhaus Advisors. 2022. Interest in Augmented Reality (AR) in the United States as of October 2022, by Age. (2022). Retrieved Feb. 2024 from https://www.statista.com/statistics/1200827/augmented-reality-interest-in-the-united-states/.
[72] Vorhaus Advisors. 2022. Interest in Virtual Reality (VR) in the United States as of October 2022, by Age. (2022). Retrieved Feb. 2024 from https://www.statista.com/statistics/456810/virtual-reality-interest-in-the-united-states/.

Appendix

A Interview Protocol

For our semi-structured interviews, we used the following protocol. The interviews lasted on average 25 minutes. Once the participant gave informed consent to the audio recording, we started recording, then started the interview. Note that the titles of the interview sections were not given to the participants and were only of use to the researchers.

A.1 Data Collection

Interview start. Thank you again for your participation. You had to experience our application with two devices, first with the [DEVICE 1], and then with [DEVICE 2]. Now I would like to start from the beginning of the experiment. When you started the experiment by pressing the "join virtual tour", you had a few permission requests. On the [DEVICE 1] you had to give access to [DEVICE 1 PERMISSIONS]. And on [DEVICE 2], you had to give access to [DEVICE 2 PERMISSIONS].

(1) To what extent did these permission requests make you question data collection aspects?
   (a) **(If permissions were refused):** What were your reasons to refuse the permissions?
   (b) **(If permissions were refused):** What were your expectations regarding the app? Did you think it would still work?
(2) What types of data do you think were collected during this experiment? **Note all mentioned data types.**
(3) For which functionalities do you think these data are needed? **Repeat for all mentioned data types.**
(4) How sensible do you think these collected data are? **Repeat for all mentioned data types.**

A.2 Privacy Settings

Now, I would like to talk about your choices regarding the settings of the application. During the experiment, you were encouraged to show your name by opening the settings page.

(1) What were your reasons for [AGREEING/REFUSING] to show your name?
   (a) **If refused:** Did you still open the settings page during the experiment?
   (b) **If they did not open settings:** Is there a reason why you did not open the settings page? **Go to next section.**

(2) What other settings did you consider when visiting the settings page?
   (a) **If they did not look at other aspects:** Can you think of a reason why?
(3) What motivated your choices when interacting with the settings page?
(4) Would you like to see other features on this page?

A.3 Comparison With Other Devices

Lastly, I would like to compare your experiences with the two different devices.

(1) How different was your experience when using the application on different devices?
   (a) I would like to compare your experiences on different aspects. For example, how different were your experiences in terms of safety?
   (b) What about the ease-of-use?
   (c) What about the immersion / the feeling of being in a different place?
   (d) What about the feeling of self-consciousness / of being conscious of your body?
(2) How concerned do you feel about your privacy when using [DEVICE 1/2]?
(3) Do you feel concerned about specific privacy aspects for this particular device?
   (a) How did you perceive the camera usage of the device?
   (b) How did you perceive the microphone usage of the device?
   (c) **For MR:** How did you perceive the eye tracker usage of the device?

   Restart from Q2 with second device
(4) If you had to compare your privacy concerns between those two devices, how would you weight them?
(5) If you had to compare those XR technologies with something more traditional, like a laptop or a smartphone, how would you weight them in terms of privacy concerns?

A.4 General Privacy Questions

(1) To what extent do you feel concerned about your privacy with Extended Reality technologies (AR/MR/VR)?
(2) To what extent did you think about privacy aspects during the experiment?

End of Interview. For you very much for your answers and your time. I will now stop the recording.

B Code Book

Table 6: Code book used to analyse our semi-structured interviews. Deductive codes are highlighted in blue.

Theme	Sub-th.	Code	Example
Permission Requests	Mental Model	Granting permissions without thinking	"But did I question myself? No, I don't think so. It's more reflex."
		Asking permissions is annoying	"Well, they're a nuisance."
		No questioning of data collection	"I didn't really think about data, my data"
		Used to apps asking for permission	"Usually my apps on my phone ask me to [...] grant access as well."
		Permissions do not cover security aspects	"These permissions I gave don't have anything to do with these [passwords]."
		MAR permission choices are misunderstood	"I will allow you while using the application, not tracking all the time."
		Lack of granular control for front and back camera	"If like, there was more [...] granular control of the different cameras [...]"
		Lack of camera permission in MR/VR is detrimental for awareness	"In the phone, I could actually see that, "Okay, the camera setting is on"."
		MR permissions catch more attention	"I guess I read it [the information on the HoloLens] more carefully"
		Assumption that apps should work without certain features/perm.	"I mean, it should work without any audio features, so I would hope so."
		Assumption that it is necessary to say yes to use app	"If you disagree, the application will not start. So what choice do you have?"
	Decision	Yes to all (only this time)	"I'm kind of trained to always use 'just this once'"
		Yes to all (while using the app)	"[...] I say 'while using the app', it's usually fine for me."
		No to all	"At first I didn't know what it was for [the permission request]."
Data Collection Awareness	Types of Collected Data	Audio	"Well, there's obviously my voice. "
		IP address	"Maybe [...] the IP address."
		Location (GPS)	"And maybe some GPS data."
		Position/Rotation	"I think, from my [...] orientation, where I was going."
		Movement	"You could probably track where I'm walking as well"
		Name	"I gave my name, in both cases, so my real name."
		Demographic data (e.g., gender, age, size)	"Maybe a profile of something like projection of my height."
		Eye tracker	"And eye tracking, maybe..."
		Video	"The camera [of] the smartphone to know [...] where I am in the real room"
	Usage of Collected Data	Communication with RE agent	"I was talking to Hannah. So [...] they had to use the microphone."
		Compute position/orientation in the VW	"Camera for maybe tracking the motion or showing the image in the background."
		Points of interest	"Maybe to see like, what I was specifically interested in."
		Video (front): facial expressions	"I think the face, um... not emotions, but expressions, I think?"
		Improving services/experience	" I think, to make the experience a little bit better [...]"
		Marketing/advertising	"To see [...] what are the objects in the environment that appeal to me in a way."
		UI interaction	"Eye tracking... yeah, is necessary to know in... [where] I tap."
		Research	"I suppose you could do something on speech and behavior and psychology"
		Other use	"Like how many people from this region are using the application."
	Sensitivity of Collected Data	Audio: sensitive	"My voice I would consider more personal."
		Audio: not sensitive	" I think my voice is not that sensitive."
		Movement: sensitive	"You can [...] find out how people move, [...] or maybe what diseases they have [...]"
		Movement: not sensitive	"I don't care about my movements, really"
		Location: sensitive	"If I have to allow all the time, then I think they are like tracking where I'm going."
		Name: not sensitive	"I think it's also, yeah, not too private to me because, yeah, it's just my name."
		Video (front): sensitive	"If it records the front camera, if it recorded me doing that, I would be very suspicious."
		Video: sensitive	"When this data will be used to analyze my real room [...] then it's very problematic."
		Video: not sensitive	"The video recording. I wouldn't consider that too sensitive."
		General: sensitive	"I suppose [...] you can look through me like a window."
		General: not sensitive	"I don't care, really. About that. I think it's fine."
		Eye tracker: not sensitive	"The eye tracking. Hmm. I don't think so. I don't think it's that much sensitive [...]"
		Eye tracker: sensitive	"Yeah, this eye tracking is, I mean, it's so special. It's very personal and so special."
Reflection on XR Experience	Missing Settings	Re-adjust the virtual room	"Maybe like a setting to, [...] go back to the start and re-adjust the room"
		Display tutorials again	"Sometimes you can't understand all the [...] controls. So maybe settings could have [them] as well."
		No suggestion	"I couldn't think of anything that was missing, so..."
		Other settings	"On the settings page there? [...] I could not change my own avatar or something like that."
	Safety	Avoiding virtual obstacles in real life	"I suddenly noticed I was about to run into a virtual wall [...] I reacted by staying back."
		Avoiding real-life obstacles	"I was a little bit afraid to bump up with the chair."
		MR can be confusing/dangerous	"I sometimes couldn't see details as well when it was too bright. So that was kind of confusing."
		VR can induce motion sickness	"So I have to say I felt like a bit motion sick with those ones [VR headset]."
		MAR as safe as MR	"I think I felt safe on both ones."
		MAR safer than MR	"Um, yeah, maybe a little bit safer with the smartphone [...]"
		MAR as safe as VR	"For the phone, I didn't have any worries about safety [...] For the headset, [...] I didn't really worry."
		MAR less safe than VR	"I think VR seems more safe because you're restricted to the same space."
		MAR safer than VR	"I suppose the thing where you can't really see where you walk, [...] is less safe."
	Ease of Use	MAR as easy as MR	"Yeah, I was at ease. I mean, in both, both applications pretty much the same."
		MAR easier than MR	"I found it easier on the smartphone because it's something one knows more."
		MAR less easy than VR	"For that I like the VR more so I could turn around and I see everything without moving a phone [...]"
		MAR easier than VR	"I think the the AR one is more intuitive [...]"
		Ease of use: unclear	"I think it was a lot more fun with the helmet, but... Sometimes it felt like a little bit dangerous."
	Immersion	MAR less immersive than MR	"When I put on the helmet, I felt like I was really in this room [...]"
		MAR less immersive than VR	"I think the virtual reality provides me with a more immersive [...] experience."
	Self-consciousness	Self-consciousness: unclear	"I don't know. I think I wouldn't be any, like conscious, or something, about it."
		More self-conscious (body) in MAR than in MR	"Yeah, I think with, um, the smartphone, I felt more in my body or more aware of it [...]"
		More self-conscious (body) in MR than in MAR	"Yeah. Um, not fully, but much more than with the smartphone."
		More self-conscious (body) in MAR than in VR	"For the headset. Uh, I guess it was like not having a body."
		More self-conscious (body) in VR than in MAR	"In VR, I was conscious, more conscious about my body because the movement was restricted [...]"

Theme	Sub-th.	Code	Example
Privacy Perceptions and Behaviour	Privacy Perceptions of MAR	General: not or little concerned (MAR)	"I think I'm a little bit naive when it comes to that because I'm not concerned."
		General: somewhat concerned (MAR)	"Um, a little. But not too much. I think with the phone I could still control enough [...]"
		General: very concerned (MAR)	"I am concerned. I know it tracks much more than I know."
		Camera: not or little concerned (MAR)	"It's also [...] tracking the camera and where you're holding the phone [...] But I did feel less concerned."
		Camera: somewhat concerned (MAR)	"The fact that [...] my phone [...] has the camera, of course, it concerns me in some kind of way."
		Camera: very concerned (MAR)	"This fear [of voice tampering] is there. But not so much than the fear of the cameras."
		Camera (face): somewhat concerned (MAR)	"But the front facing camera, I don't know, if it was recording, I wouldn't like this too much."
		Microphone: not or little concerned (MAR)	" I'm not really that concerned about the microphone [...]"
		Microphone: somewhat concerned (MAR)	"I think microphone [...] I worry more about the content, [...] like the conversation we're having."
	Privacy Perceptions of MR	General: not or little concerned (MR)	"But in this regard, no, it was more like a game for me, so I didn't really care."
		General: somewhat concerned (MR)	"Actually, I think this is more dangerous because [...] one could definitely spy things [...]."
		General: very concerned (MR)	"If I would, like, wear it on a more regular basis, I'd be much more concerned."
		Camera: not or little concerned (MR)	"No, I didn't [think] about it and I didn't know that there are cameras."
		Camera: somewhat concerned (MR)	"You would have been able to see my whole home because I basically [...] looked everywhere."
		Microphone: not or little concerned (MR)	"Not that problematic because [...] in other applications [...] you got the audio data all the time."
		Microphone: somewhat concerned (MR)	"Generally it's a bit of a privacy problem because microphones are harder to just cover than a camera."
		Eye tracker: not or little concerned (MR)	"The eye tracking was... I don't know, no problem. I don't know what anyone [...] should do with that."
		Eye tracker: somewhat concerned (MR)	"There is like, some, I'd say, inherent or subconscious concern about the eye tracking [...]"
		Eye tracker: very concerned (MR)	"I would be very aware, like when I'm on Instagram or something, when they see on which picture I look."
	Privacy Perceptions of VR	General: not or little concerned (VR)	"I would say I feel less concerned because it feels like it's less connected to my phone."
		General: somewhat concerned (VR)	"So maybe I would [...] be concerned about my privacy, but not, you know, at the at the level that I would be conscious about that [...]"
		General: very concerned (VR)	"Guess in the back of my head, I would be concerned. Like the fact that it's called the Meta Quest? [laughter]."
		Camera: not or little concerned (VR)	"It doesn't have a front facing camera, so I don't have to be worried about it filming me."
		Camera: somewhat concerned (VR)	"I think microphone is okay. But the camera..."
		Camera: very concerned (VR)	"If it's constantly recording your home, I guess there's a lot of data that can get from that [...]"
		Microphone: not or little concerned (VR)	"I think microphone is okay."
		Microphone: somewhat concerned (VR)	"Pretty much the same [as with cameras, i.e., somewhat concerned]."
		Microphone: very concerned (VR)	"For that, I would be pretty concerned, honestly. [...] More than for a phone."
	Comparison of XR Privacy Perceptions	MAR as concerning as MR	"I think I feel just as little concerned."
		MAR less concerning than MR	"I think I'm a little bit concerned with the HoloLens, but the smartphone, I don't really care."
		MAR more concerning than MR	"[With the Hololens] I felt totally safe. [With the AR Smartphone], the thing with the camera was a bit weird."
		MAR as concerning as VR	"It would be the same."
		MAR less concerning than VR	"Instinctively I would be more concerned with the headset than the phone."
		MAR more concerning than VR	"I would [be] more concerned with my smartphone because [...]"
		No differences in perception of cameras	"The phone [...] scans your surroundings, but I think it's, like, the same with the helmet"
		No differences in perception of microphone	"Like, the microphone thing is the same. It was like the smartphone usage."
		Differences in perception of microphone	"Yeah, I suspect there's a difference because this is more modern."
		Differences in perception of eye-tracking vs camera	"I guess it can eye track, whereas I suppose the smartphone does not eye track."
		No differences in perception of eye-tracking vs camera	"Like with the phone. It scans your face and your eyes too. But with the helmet, it scans your eyes as well."
		Differences in perception of movement	"With AR you had to move around, and with the other one, you were standing still kind of."
		General: very concerned (XR)	"Yeah, the experience is much better, but [...] the [collected] data are much more real."
		General: somewhat concerned (XR)	"With all of these new technologies, they can collect data and you sometimes don't know about it."
		General: not or little concerned (XR)	"I'd say also very little. Um, to me, it's just like a bunch of data [...]"
	Comparison of XR vs. Traditional Technologies	MAR app as concerning as normal smartphone app	"I feel like it's just the same as when I'm using FaceTime or my camera app"
		MAR app more concerning than normal smartphone app	"I guess I would be more concerned with the augmented reality software"
		XR as concerning as traditional technologies	"I would weight them the same, I think [...]"
		XR less concerning than traditional technologies	"In general, less concerned with these augmented and virtual reality stuff."
		XR more concerning than traditional technologies	"When I scroll through [a] computer, they are collecting much less data than [AR smartphone and HoloLens]."
	Privacy Behaviour	Resignation due to data already being everywhere	"I think my voice is not that sensitive. I have the feeling that it's already everywhere."
		Not giving data if not mandatory	"I don't like to put my data somewhere where I don't have to in some way."
		Concerns are forgotten once decision to use the device/app is made	"If I like, decide to use it then I don't really think about it [...]"
		Context of study lowers concerns	"And at the moment, in this experiment, I feel very safe that, um, the data is not going anywhere."
		Mention of privacy trade-off	"I think it's always a compromise between the comfort I want to have playing a game [...] and privacy issues."
	Privacy Concerns	Unconcerned about data collection	"There are so many people using it and it all comes together and [...] No one cares about my data."
		Unconcerned about targeted advertising	"We're getting ads anyway, if it's ads that actually would please me, I'm okay with it."
		Unconcerned about spatial data	"If it's just like, broken down data just about like, where are objects in your room, that wouldn't concern much."
		Unconcerned because avatar is shown in their place	"I can see the avatar, not exactly what I am appearing like, [...] so I think it's not a big deal."
		Concerned about replication of body movements on avatar	"I wasn't sure [...] if she would see my body move as well [...] I was a bit insecure about that."
		Concerned about biometric data	"Maybe it could have scanned my eye, like the biometrics of it. And that could be, um, a safety problem, maybe."
		Concerned about filming of private environment	"Maybe I would be more uncomfortable if I was at home and someone could see that."
		Concerned about security of financial data	"I would only be concerned about [...] financial things? Like if you can find passwords to my bank account"
		Mention of lack of transparency regarding data collection	"I need to trust Apple that they actually don't listen to the microphone. But if they would, I would not have any way to find that out."
		Mention of privacy invasion regarding advertising	"If I was interested in the towel holder, my guess is the next time I open Google, I get commercials about towel holders."
		Mention of mass surveillance	"I know like in China, everything is tracked. [...] We're not far from that."
		Mention of covers on cameras	"I think a lot of people are, like, covering their camera."

Theme	Sub-th.	Code	Example
Privacy Perceptions and Behaviour	Privacy Mental Model	Immersion in MR/VR distracts from privacy concerns	"It provides me with a more immersive experience. So I kind of forget where am I and [...] I don't really think about the private things when I'm using it."
		Assumption that XR devices are more modern, therefore collect more data	"I would view the headset as a device with the purpose of collecting my data somewhat more than a phone."
		Concerns depend on involved parties	" I mean, even, like, Google, for example, could do something [...]"
		Concerns depend on presence of bystanders	"Google glasses were a thing. [...] I could go into the city and use [the HoloLens] there. Then it suddenly would become an issue."
		Concerns depend on knowledge of technology	"I don't know what anyone [...] should do with [...] my eye tracking."
		Concerns depend on context rather than nature of data	" Not that much because it kind of made sense in the moment that an app that allows me to talk to someone would need access to the microphone."
		Concerns depend on data collection purpose	"Is it used for something else than that? And can I like, choose for what it is used?"
		Concerns depend on trust that permission requests are respected	"I think it should be okay if I only have to give permission when using it and then it cannot use it if I don't allow it, then it should be okay."
		Concerns depend on amount of personal data present on the device	"So like, my phone has, like, this whole profile of me and I'm doing everything on my phone."
		Concerns depend on ownership of device	"If it is mine, then I will feel more safe. If it is others then yeah the privacy issue matters."
	Self-disclosure of Personal Information	Name asked by REA	"I did it because I was asked to do it."
		No reason to refuse	"I had no no reason to not do so. "
		One on one conversation	"It was only like a one on one conversation with someone [...]"
		Name was already in the application	"The data was there already, I guess. The only person who couldn't see it was Hannah."
		Wanting an equal to equal interaction	"It just made sense to me because she was also showing her name and I wanted to have like a normal interaction, like equal, I guess."
	Awareness During Experiment	Not at all	"Not at all."
		Almost not	"I would say almost not."
		A bit	"A bit. Yeah."
		Awareness during task of showing name	"I was just thinking for a moment also with the name [...]"
		Awareness during ET calibration	"Maybe with the HoloLens as you tracked my eyes? As it tracked my eyes."
		Awareness during permission requests	"So, first only at the moment when they were asking me, "can I use your camera" [...]"
		Awareness about privacy in general	"I can never be sure, absolutely sure. So I for myself try to never trust anything completely."
	Behaviour Regarding Settings	Other setting was considered	"Yeah, there was another, uh, setting on which you, Uh, you could... I think mute yourself."
		Other setting was not considered	"Uh, there was one box underneath, but I didn't read, to be honest."
		Reasons for not considering other settings: setting was off	"If I spotted one that was turned on by default, I would have looked at that."
		Reasons for not considering other settings: no reason/was not asked to	"Because I wasn't asked to."
		Reasons for not considering other settings: concentrated on current task	"I just wanted to make the progress and show my name."
		Motivations for opening settings: task of showing name	"She asked me to display my name."
		Motivations for opening settings: curiosity	"I was curious, I think."
		Showing name by anticipation the 2nd time	"I thought, "Oh yeah, she's going to ask me, so just do it now"."
Understanding of Technology		Low knowledge of XR	"I don't know much about HoloLens or Augmented reality."
		Awareness that voice can be tampered with (e.g., AI, out of context)	'They could make [...] this AI stuff so it can fake your voice and do [...] something with that.'"
		Uncertainty about frontal or back camera use	"I don't know if the cameras in front... was used, whether the camera was used."
		Lack of understanding about necessity of camera to track planes in XR	"I think that's a spy thing. I don't see any reason why that should be there [laughter]."
		Virtual behaviour based on existing technologies (e.g. 2D video calls)	"Like when I would see the other person too, like in a zoom meeting or something like this [...]"
		Unaware about presence of sensor on device	"No, I didn't [think] about it and I didn't know that there are cameras."
		No distinction in sensor usage by OS vs by app	"You can use the gyroscope to know if I move my head or something."
		Assumption that front camera is not used	"Well, it can't see me."
		Assumption that VR has eye tracker	"I think eye-tracking information might have been collected [...] for the VR for sure."
		Assumption that VR doesn't track surroundings	"It fully submerges you in another virtual reality, so there's like no tracking of your surroundings, right?"
		Assumption that XR devices are only meant for one thing (e.g., gaming)	"This headset is only meant for one thing, whereas the phone [...]"
		Confusion of terms (MAR/MR/VR)	"The [Hololens] was very confusing because it [...] immerses you [...] in this virtual reality thing."
		Expectation of HW features in settings (e.g., volume, brightness)	"I would probably look further [...] for contrast or light [...]"
Miscellaneous		Possibility of mixing real world and virtual world better in MR	"On the HoloLens, I could kind of focus my eyes differently to see either the virtual or the real environment at the same place."
		Behaviour in virtual world inherited from real life social customs	"Even if I knew this was a virtual person there, I always had the same, you know, standing away from a person then... like this would be a real person [...]"
		Mention of discrimination in XR experiences	"That could lead to quite a few discriminations [...]"
		MR has a higher cognitive load (concentration on both realities)	"I have to watch at both rooms at the same time. And I think I needed a bit more concentration for this."
		App is rudimentary	"It was a very rudimentary settings page."
		Looking dumb while wearing a headset	"I thought maybe I'm looking totally dumb with this."
		Avatar has unrealistic arms placement	"The avatar I was seeing [...] sometimes twisted their arms in impossible ways."