Designing Privacy Interfaces for Informed Consent in Virtual Reality: Challenges and Design Implications

Viktorija Paneva
LMU Munich
Munich, Germany
viktorija.paneva@ifi.lmu.de

Verena Winterhalter
LMU Munich
Munich, Germany
verena.winterhalter@ifi.lmu.de

Naga Sai Surya Vamsy Malladi
University of Bayreuth
Bayreuth, Germany
Naga.Malladi@uni-bayreuth.de

Evgeniia Maltseva
LMU Munich
Munich, Germany
e.maltseva@campus.lmu.de

Marvin Strauss
HCI Group
University of Duisburg-Essen
Essen, Germany
marvin.strauss@uni-due.de

Stefan Schneegass
HCI Group
University of Duisburg-Essen
Essen, Germany
stefan.schneegass@uni-due.de

Florian Alt
LMU Munich
Munich, Germany
University of the Bundeswehr Munich
Munich, Germany
florian.alt@ifi.lmu.de

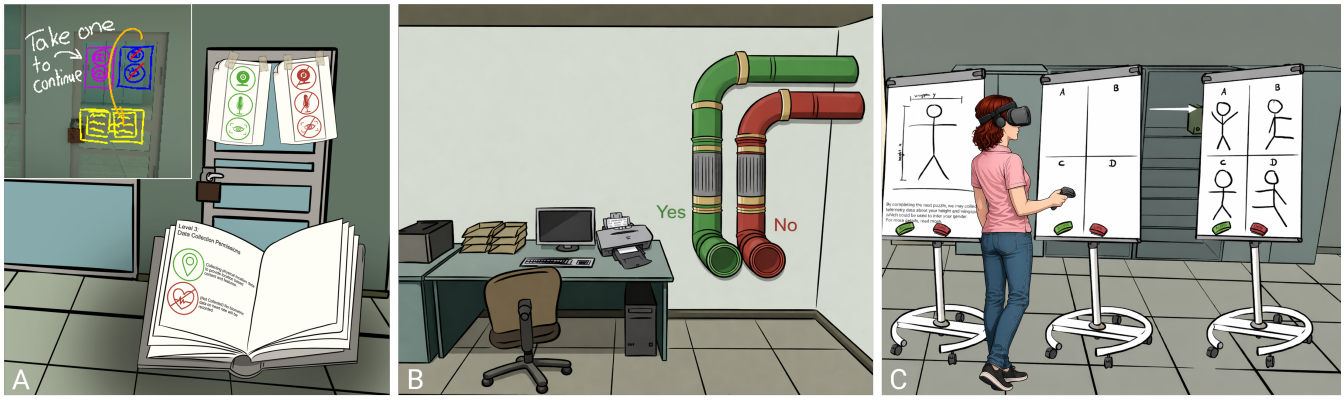

Figure 1: Design concepts for data collection awareness and control in Virtual Reality (VR), developed through participatory design sessions and refined with expert feedback. We explore how spatial and embodied interactions in immersive environments can support data awareness and user control, particularly when using data-intensive devices, featuring always-on sensors such as head-mounted displays (HMDs). (A) *Sticker Book* enables granular, purpose-tied permission management and was implemented as a high-fidelity VR prototype for exploratory user evaluation. (B) *Privacy Post* presents a privacy notice on a screen that players can print, review, sign, and submit via color-coded pneumatic tubes, enabling embodied consent interactions. (C) *Consent Canvas* is a whiteboard interface that offers explicit accept/deny actions, which can trigger alternative, data-minimizing tasks.

Abstract

Virtual Reality (VR) headsets rely on arrays of sensors that continuously collect fine-grained user and contextual data, which is often undisclosed or poorly explained in privacy policies. We investigate how VR's spatial and embodied affordances can support data collection awareness and control through interactive privacy interfaces. Using a mixed-methods, design-led approach, combining participatory design sessions, expert feedback, and an exploratory user evaluation, we generate and refine a set of VR privacy interface concepts, identify key design tensions, and derive design implications highlighting privacy-preserving defaults, granular and revisable consent options, continuous feedback, and thoughtful gamification.

NordiCHI '26, Vaasa, Finland

ACM ISBN 979-8-4007-2373-5/26/10
https://doi.org/10.1145/3829807.3829825

We operationalize these implications in a high-fidelity VR prototype (the *Sticker Book*) and explore how users experience granular control options, contextual permission prompts, and ambient indicators during interaction. Our findings show how these mechanisms work together when embedded in a functional VR application, revealing practical trade-offs between transparency, user control, and presence, and providing practical guidance for designing for informed consent in sensor-rich immersive environments..

CCS Concepts

• **Human-centered computing** → **VR**; • **Security and privacy** → **Usability in security and privacy**.

Keywords

Usable Privacy, Informed Consent, Virtual Reality (VR), Extended Reality (XR), Interaction Design.

ACM Reference Format:
Viktorija Paneva, Verena Winterhalter, Naga Sai Surya Vamsy Malladi, Evgeniia Maltseva, Marvin Strauss, Stefan Schneegass, and Florian Alt. 2026. Designing Privacy Interfaces for Informed Consent in Virtual Reality: Challenges and Design Implications. In *Proceedings of the 14th Nordic Conference on Human-Computer Interaction (NordiCHI '26), October 03–07, 2026, Vaasa, Finland*. ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3829807.3829825

1 Introduction

Sensors in Virtual Reality (VR) hardware bring data collection close to the human body. Compared to 2D platforms, VR headsets rely on a wider range of sensors that continuously capture fine-grained behavioral, physiological, and contextual data for tracking and interaction. Beyond enabling core functionality, such data can be used to uniquely identify users and infer sensitive information. Prior work shows that user identification based solely on VR sensor data can reach very high accuracy [16], while telemetry and eye gaze data can be indicative of users' well-being, literacy, impairments, political views, and gender [31, 48]. Furthermore, users are often unaware of the extent of these capabilities, including the capture of involuntary body signals indicative of emotions [13]. This can invade users' privacy, allowing third parties to obtain information users might not want to share.

Despite regulatory requirements such as GDPR[1], which mandate transparency and informed consent, current VR privacy practices remain limited. Audits of VR applications have shown that a large portion of data flows are not properly disclosed, and that collected data is frequently used beyond the app's primary functionality [51]. Further studies characterize VR policies as of poor quality, coarse-grained, and lacking adaptation to VR [55]. These issues compound known challenges of privacy policies and permissions in 2D interfaces (e.g., smartphones [38]), including (1) important information being often inaccessible to users due to being buried in pages of legal text [15, 33] and (2) users typically having a limited understanding of how their privacy-related decisions affect later app use [50]. Recent work suggests that these challenges extend to immersive technologies, where users frequently misunderstand why mobile AR applications request particular permissions and how those permissions relate to app functionality [36]. In VR, these challenges are further complicated by continuous sensing and the tight coupling of system functionality with ongoing data collection.

Together, these challenges motivate rethinking how data collection awareness and control can be supported in VR, where its spatial, interactive, and embodied affordances may enable alternative ways of communicating and enacting consent.

In this work, we explore how such affordances can be leveraged to design privacy interfaces that support data awareness and user control in VR. We adopt a mixed-method, design-led approach, combining participatory design sessions with novice game designers and developers, a focus group with privacy experts, and the implementation and exploratory evaluation of a high-fidelity prototype. Through this process, we generate a set of VR privacy interface concepts, identify key design challenges, and derive design implications for supporting informed consent in immersive environments.

The research questions guiding our work are:

- RQ1 How can privacy interfaces in VR be designed to support informed consent? *(design goals)*
- RQ2 What challenges do developers and designers face when creating such interfaces? *(practical challenges)*
- RQ3 What design implications can guide the development of data collection awareness and control mechanisms in VR? *(implications)*

Contribution Statement. Our contributions are threefold:

(1) **VR Privacy Concepts and Expert Evaluation**: We present a set of novel low- and high- fidelity interface design concepts for informed consent in VR, developed through participatory design and refined through expert feedback.
(2) **Design Implications**: We derive actionable design implications for data collection awareness and control in VR, grounded in design sessions, expert feedback, and prototype exploration.
(3) **Prototype Implementation and Exploratory Evaluation**: We implement a high-fidelity VR prototype[2] (*Sticker Book*) and conduct an initial user study to explore its feasibility, usability, and user experience.

2 Related Work

Our work draws from several strands of prior research, spanning traditional privacy mechanisms for 2D interfaces, and data collection and privacy considerations in Extended Reality (XR).

2.1 Data Collection in XR

XR headsets utilize an array of sensors (including multiple always-on cameras) that bring data collection closer to the human body, enabling sensitive data to be captured, processed, and shared with third parties. State-of-the-art headsets provide access to behavioral data (e.g., hand and body motion, eye gaze), physiological data (e.g., electroencephalography, heart rate), contextual data (e.g., size of tracking space, bystanders), and device specifications [11, 31]. This introduces new risks: for example, the GAZEploit [53] cyberattack exploits gaze data to steal sensitive keystroke information. Furthermore, sensor data can be used to make inferences

[1] GDPR: https://gdpr-info.eu/

[2] https://github.com/EvgeniiaMaltseva/PrivacyPermissionsUserStudy

about user attributes, such as demographics (e.g., age, gender, handedness), health and well-being (e.g., reaction times, fitness level), impairments (e.g., visual or motor impairment), and emotional state [31, 48, 49]. While these data also enable valuable features for XR users (e.g., seamless interaction) and stakeholders (e.g., target ads), they carry severe privacy implications [6]. A comparative analysis of the network traffic from VR applications found that approximately 70% of the data streams were not adequately disclosed in the privacy policies, with the ecosystem – other than in mobile – more driven by data and analytics than third-party advertising [51]. In response to such risks, Adams et al. [3] proposed a code of ethics advocating for secure protocols, transparency in data collection, and obtaining user permission each time data is collected. However, guidance on implementing these principles in practice is still lacking.

2.2 Data Collection Awareness

Different approaches exist to improve user awareness of data collection. Kelley et al. [17] proposed the idea of "nutrition labels" for privacy, which communicate what data is collected, how it is processed, and whom it is shared with. This idea has been appropriated for specific application areas by both researchers and companies, for example, as part of Apple's iOS 14. However, recent investigations showed that these can often be inaccurate and misleading, with discrepancies between the data disclosed in the apps' nutrition labels and actual data practices [21]. Beyond static disclosures, prior work has explored tools that provide more contextualized awareness of data collection. PriView [39] identifies data-collecting sensors in smart homes through visual and heat signatures, displaying the tracking space on a smartphone or a head-mounted display. PriCheck [52] is a browser extension providing privacy-related information about smart devices. Finally, privacy dashboards, such as Google's My Activity[3], have been introduced to help users review and manage data collected online. While it has been shown that privacy dashboards primarily support trust, their actual benefit in improving users' privacy remains unclear [8].

2.3 Control Mechanisms

Prior work investigated how users can be given control over data collection. The most common approach to gathering consent is notice and choice [47]. However, notices often suffer from poor usability [45]. Users generally do not know when and which data is collected. Furthermore, setting privacy permissions does not scale, leading users to quickly give up on managing which sensors/data each app and service should have access to [38].

Researchers proposed visually appealing privacy notices [19] and notices considering timing, functionality, and modality [10]. Morrison et al. [30] showed that users confronted with visual representations of collected data by smartphone apps became more concerned and often stopped app usage sooner. Studies on user behavior when granting permissions explored visual cues to support decision-making [42], and statistical insight to improve understanding of the implications of consenting to permissions [22]. King et al. [18] showed that designing privacy choices to be personal and concrete supports users' privacy decisions. Momen et al. [29] introduced partial consent, adding an indecisive state that allows users to evaluate data services before providing full consent. Similarly, an approach beyond binary permission options was proposed as a fine-grained privacy permission slider for AR applications [1]. Despite substantial work on privacy control mechanisms, it remains unclear how to design for informed consent in VR environments, characterized by continuous sensing and embodied interaction.

[3]Google MyActivity: https://myactivity.google.com

2.4 Usable and Privacy-Preserving XR Interactions

The design of XR interactions often prioritizes usability and feasibility at the expense of security and privacy. Recent work has sought to address this imbalance by embedding privacy and security concerns into development processes, aligning the expertise of XR developers and privacy experts. For example, Rajaram et al. [40] employed scenario-based threat modeling in multi-user AR to balance competing goals of usability, feasibility, and security/privacy. Ruth et al. [46] proposed design goals that accommodate security needs while maintaining functionality, exemplified by a content-sharing prototype for multi-user AR. Tools like *SecSpace* [43] and *Reframe* [41] further assist developers identify security and privacy risks early in AR/MR design. While methodologically relevant for our study, these approaches primarily focus on design-time analysis and offer limited guidance on user-facing interaction and interface design for supporting informed consent.

2.5 Summary

Privacy challenges in XR are distinct due to the presence of (always-on) sensors, fine-grained data collection, and their proximity to the user's physical body, allowing the collection of potentially sensitive personal information. While previous studies on 2D interfaces propose approaches for data collection awareness and control, such as privacy labels or assistants, these often fail to provide users with a sufficient understanding of when and why data is collected or the implications of their choices.

HMD-based VR systems introduce additional complexities by combining environmental, physiological, and behavioral data, including eye-tracking, hand movements, and body posture, revealing sensitive information such as emotions, health conditions, or identity [31, 32, 37]. These challenges, acknowledged by researchers and industry [2, 3, 13, 35], highlight the need for privacy interfaces tailored to VR contexts and interaction paradigms (**RQ1**).

Existing tools such as *SecSpace* [43] and *Reframe* [41] facilitate integrating privacy considerations in multi-user MR and AR interactions. However, there is limited systematic research on the practical challenges of designing user-facing privacy interfaces for HMD-based virtual environments. Understanding these challenges is critical to bridging user needs and implementation constraints, motivating our focus on designers' and developers' perspectives (**RQ2**).

Prior work further highlights that incorporating privacy considerations into XR systems often requires balancing competing design goals, such as usability, feasibility, and privacy [40]. This underscores the need for actionable, design-oriented guidance for

developing privacy mechanisms in VR that balance usability, transparency, and compliance (**RQ3**).

3 Research Approach

We employ a mixed-method approach consisting of concept brainstorming and sketching sessions with novice game designers and developers (Figure 2A), a focus group with usable privacy experts (Figure 2B), and prototype implementation and evaluation with end users (Figure 2C). Together, these stages inform the generation and refinement of design implications for data collection awareness and control interfaces in VR (Figure 2D). Our approach builds on methods in prior work, such as the user-centered design process employed by Fassl et al. [9] for developing authentication ceremonies for instant messaging, and the involvement of novice AR designers and security and privacy experts in formative design work by Rajaram et al. [41].

In our study, novice game designers and developers developed intuitive and engaging data collection awareness and control VR interfaces, individually or in groups (depending on availability), during think-aloud brainstorming and sketching sessions using a virtual 3D sketching tool. The 3D sketching tool allowed participants to prototype directly within the VR scene, providing a better understanding of placement, proportion, and effective use of the virtual 3D space. Studies have shown that 3D sketching can be more stimulating and engaging, especially in the early design process [14], as it promotes physical and perceptual action and enhances flexible cognitive thinking more than traditional 2D methods [26]. These live sessions allowed us to gain immediate insight into the topics and challenges that naturally emerged during the design process.

Following the brainstorming and sketching sessions, selected design concepts were refined and re-sketched for further evaluation in a focus group with usable privacy and XR experts. We made audio recordings to capture participants' discussions, observations, and insights. We transcribed and analyzed the recordings using thematic analysis. We then implemented a functional VR prototype of one proposed design and conducted an initial user evaluation to explore its feasibility, usability, and user experience.

Drawing on insights from the hands-on design sessions, expert feedback, and user evaluation, we discuss strategies for effectively integrating privacy-related information in VR and synthesize actionable design implications.

4 Concept Brainstorming and Sketching Sessions

This section describes the process of generating privacy interface concepts for VR, detailing the apparatus, procedure, participants, data analysis, limitations, and results.

4.1 Apparatus

The sketching sessions were conducted using an HTC Vive Pro HMD[4]. For the study, we adapted and extended the open-source virtual environment *MetaData* developed by Nair et al. [31] as a research-probe VR escape room experience constructed to harvest user data.

[4]www.vive.com

Given VR's widespread use in entertainment contexts and the sensitive information that can be revealed through interactive experiences (e.g., interests, emotions, and skills), [24], we selected *MetaData* as a suitable sandbox for exploring data collection awareness and control interventions, as it provides multiple examples of sensor-based data collection and inferred user attributes within an ecologically grounded yet controlled setting.

The virtual environment consists of a sequence of rooms, each associated with a specific type of data collection. In each room, participants complete an interaction that reveals a codeword while enabling collecting a particular type of user data or the inference of user attributes. To keep the design sessions within a reasonable duration and avoid participant fatigue, we presented four rooms targeting color blindness, wingspan, reaction time, and foreign language knowledge (screenshots are provided in Appendix A). Together, the rooms exposed participants to different categories of collected and inferred information (e.g., physical characteristics, cognitive performance, and personal attributes), providing participants with concrete privacy scenarios when designing awareness and consent mechanisms. Participants then selected two of these rooms for the design development.

To support in-situ prototyping, we extended the *MetaData* environment with our own custom 3D sketching tool, integrated directly into the existing Unity project. This tool allowed participants to sketch within the virtual scene by drawing freehand lines in 3D space, resizing and rotating the sketches, and performing undo actions using hand-held HTC Vive controllers.

4.2 Procedure

We began by explaining the study's purpose and procedures, then obtained signed consent for voluntary participation and audio recording. Participants completed a demographics questionnaire and then we familiarized them with the VR escape rooms and the 3D sketching tool, allowing time for practice. Once comfortable, they moved on to the main task: creating low-fidelity prototypes of data collection awareness and control interfaces within different escape rooms. Depending on participant availability, the design sessions were conducted either individually or in small groups of two to three participants. Participants working together collaboratively developed shared design concepts. They first brainstormed ideas on paper, then selected promising concepts for low-fidelity prototyping in VR, using a think-aloud protocol to articulate their design decisions as they sketched. Afterward participants took part in a semi-structured interview, where they could provide more detail on the specifics of their designs, encountered challenges, and their overall reflections on privacy considerations in VR development. The interview protocol and other user study materials are provided in Supplementary Materials.

4.3 Participants

Using convenience sampling followed by snowball sampling, we recruited 12 participants (2 females, 9 males, 1 non-binary), aged between 21 and 26 years (mean age 23.92, SD 1.56). Participants were drawn from a cohort of students enrolled in Computer Games and Media Studies programs, all with prior experience in game design. The study was conducted at a German university and all

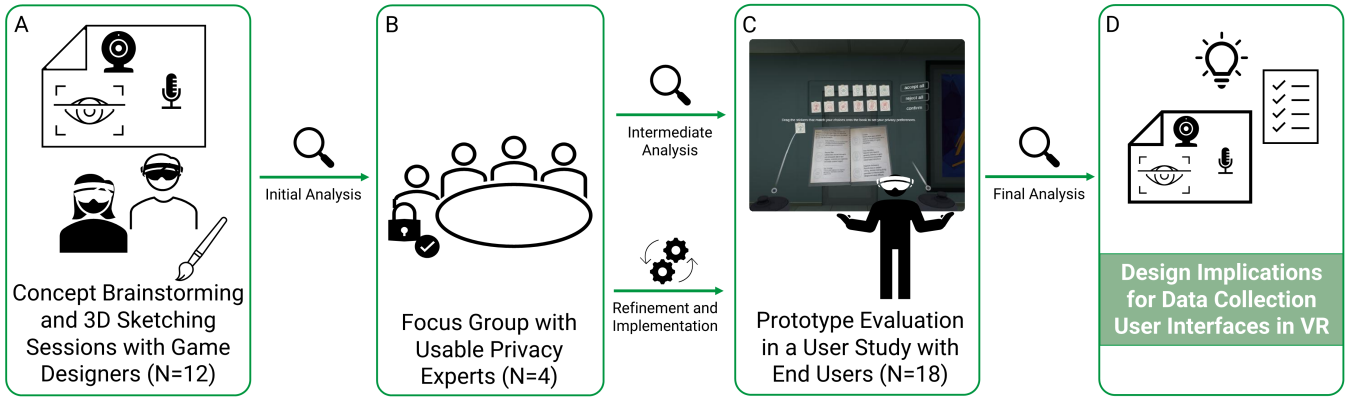

Figure 2: Overview of the research approach. (A) Novice game designers and developers ideate and sketch VR privacy interface designs in participatory concept brainstorming and in-VR sketching sessions. (B) The generated design concepts are analyzed and discussed in a focus group with usable privacy experts to assess effectiveness and feasibility. (C) We implemented a functional VR prototype and performed an exploratory evaluation with end users. (D) Design implications were synthesized primarily from the design sessions and expert focus group, and subsequently examined through the prototype implementation and user evaluation.

study sessions were conducted in English. Eligibility criteria included having completed at least one course related to game design, having worked on a game design-related project, or having professional experience in the game design industry. Ethical approval was obtained from the Ethical Committee of the University of Bayreuth (Reference No. 24-041). Each participant received €20 compensation for their participation. The study lasted approximately 90 minutes.

4.4 Data Analysis

The collected data included audio recordings of the think-aloud prototyping sessions, 3D sketches of conceptual prototypes, and audio recordings of the concluding semi-structured interviews. We collected and analyzed 395 minutes of audio recordings in total, with an average of 56.43 minutes (SD 15.59) per design session. We transcribed the audio recordings using MAXQDA transcription software and reviewed the sketches to better understand their structure and design intentions. Then we applied inductive thematic analysis [25], where two researchers independently open-coded the transcripts of a randomly selected prototyping session, accounting for approximately 15% of the data, and met to discuss the initial codes and form a common codebook. Three researchers then used the common codebook to code the remaining prototyping sessions. The three researchers iteratively compared and discussed codes in online meetings. The codes of the final codebook were jointly discussed and grouped to identify common themes. The codebooks are provided in Supplementary Materials.

4.5 Limitations

Our brainstorming and sketching sessions involved student game designers and developers who had completed at least one semester of relevant coursework. While their professional experience was limited, participants nonetheless identified challenges that have likewise been reported by more experienced practitioners in prior work, such as balancing privacy mechanisms with immersion and the lack of established guidelines and standards for privacy in VR [3]. To complement this perspective and mitigate potential gaps in expertise, we subsequently conducted a complementary focus group with usable privacy experts, including one member with XR expertise. While the focus group provided valuable interdisciplinary feedback, its small size and recruitment from our academic network may have limited the diversity of perspectives. Future work could therefore include a broader range of stakeholders, including industry practitioners and regulators.

We anchored our exploration in a VR escape room experience to provide a concrete and engaging environment for evaluating privacy interface concepts. While this approach enabled ecologically valid insights and the development of situated design ideas, certain game-specific elements may need some adjustments to extend to other VR domains. We therefore do not claim universal applicability of our scenario-based elicitation method across all XR use cases, particularly those beyond HMD-based VR. Future work could examine a broader range of scenarios and interaction contexts to further assess the transferability of the proposed concepts and design implications.

4.6 Results Design Session

The following sections detail our findings from the concept brainstorming and sketching sessions. We begin with an overview of the collected designs, followed by the themes identified in the thematic analysis of the design session and interview transcripts.

4.6.1 Designs. We briefly describe the different design concepts developed during the design sessions. A summary of all designs can be found in Table 1. Several approaches focused on informed consent mechanisms, such as displaying privacy notices on computer screens for players to sign and submit through pneumatic tubes to accept or deny data collection (D2), attaching privacy notices to the player's avatar to accept or disposing of them in virtual trash cans to deny (D4), and placing stickers in a privacy book to manage data collection permissions (D17). Other designs explored alternative

Table 1: Summary of the design concepts developed during the brainstorming and sketching sessions, encompassing informed consent mechanisms, alternative game mechanics to minimize data collection, and awareness-raising strategies. Participant ranges (e.g., P2–4) denote concepts developed collaboratively during the same design session; single participant IDs denote concepts developed individually. Abbreviations: RT = Reaction Time, W = Wingspan, L = Language.

ID	Attr.	Type	No.	Description
P1	RT	Awareness	D1	The player plays a minigame where they swat virtual bugs to raise awareness about collecting reaction time data.
P2-4	All	Inf. Consent	D2	A privacy notice is displayed on a computer screen, which the player can sign by typing their name on the keyboard and then print. To accept or decline, players place the printed document into one of two labeled pneumatic tubes on the wall: "Yes" to accept and "No" to deny data collection. A "woosh" sound confirms the document has been sent.
	W	Alternative	D3	The player can manipulate a mannequin placed in the room to display the poses needed to reveal the password.
P5-6	All	Inf. Consent	D4	A piece of paper in each room briefly informs players about data collection. Players can provide consent by attaching the paper to their avatar, similar to collecting items in games, or deny it by simply throwing it into a trash can.
P7	W	Inf. Consent	D5	The player stands in a body scanner marked by a circle on the floor, with a projector-like device above. A privacy notice appears on a display. To accept data collection, the player must mimic a pose projected by the device; otherwise, they are teleported to the next room.
	W	Alternative	D6	The room contains four mannequins that the player can adjust to match the required poses.
	W	Alternative	D7	A stack of interactive balls is placed on a table to serve as markers. The players must position these markers in mid-air to replicate the poses on the wall, revealing the password.
	RT	Alternative	D8	The player must solve a logic pattern puzzle instead.
P8	All	Awareness	D9	There are multiple cameras mounted in each room, and the red indicator light will be turned on to signify ongoing data collection to the player.
	L	Alternative	D10	The password is written on an interactive globe in the language predominantly spoken in each respective country.
	All	Alternative	D11	The letters of the password are hidden in the room; the player must search for them to find the password.
P9	All	Inf. Consent	D12	The privacy notice is written on a whiteboard. The player can exercise control by using one of the two erasers labeled "accept" or "deny".
	W	Alternative	D13	The player must draw the different poses on the whiteboard.
	All	Alternative	D14	The letters of the password are blended within other objects, requiring the player to search and identify them.
P10-12	All	Awareness	D15	A camera with a blinking red light indicates data collection.
	All	Awareness	D16	A privacy companion, e.g., a robot, accompanies the player and provides information about data collection.
	All	Inf. Consent	D17	On the door of each room, there are "accept" or "deny" stickers for each data collection type. The player exercises control by placing these stickers in their data collection book.

game mechanics to minimize data collection, such as manipulating a mannequin (D3 and D6) or drawing on a whiteboard (D13) instead of using body tracking, which would otherwise capture telemetry data, such as height and wingspan. A general alternative for all data collection tasks included hiding letters of the codeword within the virtual environment, requiring players to search for them instead, thereby eliminating direct data capture from specific interactions (D11 and D14). Awareness-raising designs included using visible cameras with indicator lights to signal active user tracking (D9 and D15) and interactive companions, such as a robot or other game character, that inform users about data collection (D16).

Having introduced the design concepts, we next examine the design process and the underlying considerations that informed these concepts. We organized the findings into three overarching themes: *Design Process*, *Challenges*, and *Properties of the Privacy Mechanisms*, summarized in Figure 3.

4.6.2 Design Process. We identified five categories in this theme: *Creating Designs*, *User Perspective*, *Designer's Role*, *Privacy Considerations*, and *Transferability*.

Creating Designs describes the designers' feedback regarding the design activity and their experience when creating the designs in a 3D environment. They mentioned that "it was very fun, (...) like a cool way of puzzle solving" (P2) while being "different than drawing in 2D" (P1), which took a bit of time initially to adjust (P1, P4).

User Perspective and *Designer's Role* reflect on how considering the user perspective informed the designs and how designers and developers perceived their roles and responsibilities regarding privacy. P6 mentioned that "if a game would sell [the data] to companies for like advertisement (...) then it is [a] concern, but to improve the game I think it is all right", and P1 added that it is "a compromise you make with yourself" when sharing data to use an application. Regarding their role as developers, participants mentioned that they "have to be aware [of the data processing] while designing the games" (P2), and the trust users place in developers, who in their role have higher awareness of these issues (P1).

In *Privacy Considerations*, we grouped the privacy aspects designers saw as important for their design. Multiple participants mentioned that privacy considerations are not something they usually think about (P1, P2, P7, P9). P1 and P7 also noted that the importance of these considerations varies with the type of game they develop and the company's size and interests.

The final category, *Transferability*, contains the designers' thoughts about how well their designs adapt to other contexts. Most designs were described as requiring adaptation, for example, to reflect specific scenarios (P2, P5, P7) or a different number of privacy choices that must be covered (P7). P5 also thought about "mak[ing the design] more basic" to fit multiple applications more easily.

4.6.3 Challenges. We identified two main themes related to the challenges designers faced: *External Challenges* and *Design Challenges*. *External Challenges* include the influence of company structures and legal requirements. P3 raised the question of which perspective is taken during the development: "Are we the company or are we pro people's data?", hinting at a possible conflict between user and company interests. While participants were aware that privacy mechanisms had to be legally correct (P3, P5), they also noted a lack of confidence in determining a legally appropriate privacy-preserving design (P3).

Design Challenges contains different aspects to be considered during the design, such as *Complexity of Privacy Policies, Usability,*

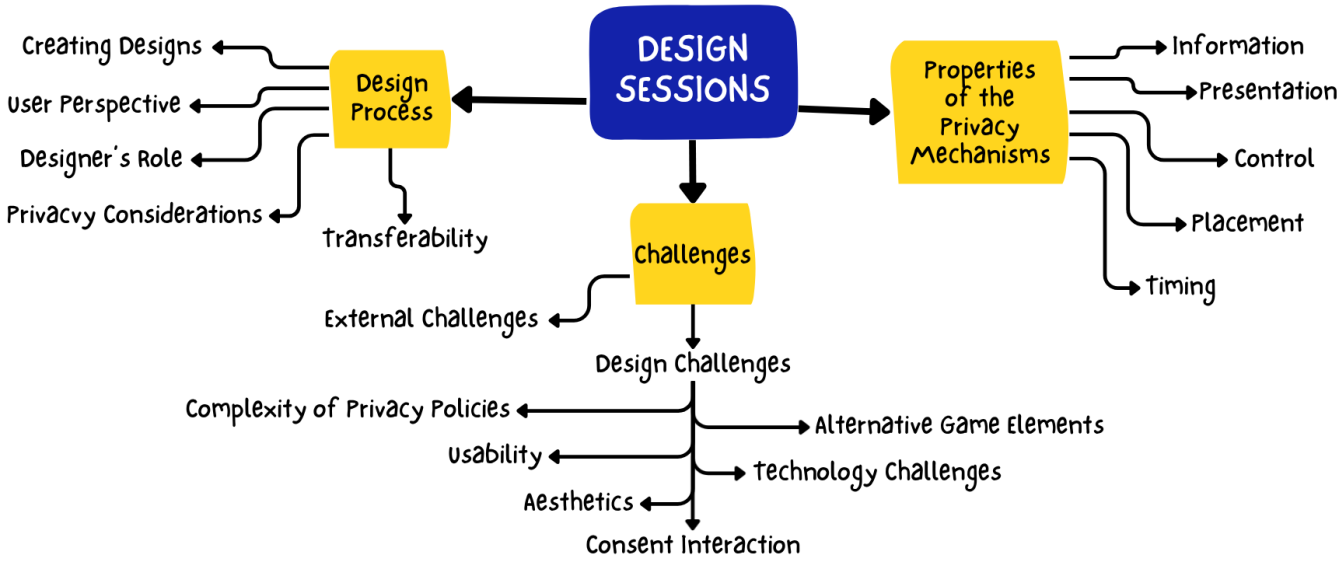

Figure 3: Overview of themes emerging from the thematic analysis of the concept brainstorming and sketching design sessions, with three main identified themes: Design Process, Challenges, and Properties of the Privacy Mechanisms.

Aesthetics, Consent Interaction, Technology Challenges, and designing *Alternative Game Elements.*

Complexity of Privacy Policies. Several factors contribute to the complexity of privacy policies, especially in VR, where a lot of privacy decisions have to be considered. Participants P4, P5, and P10 highlighted the importance of avoiding lengthy, repetitive interactions while still covering the different areas of data collection within the environment and the different rooms: "If only one type of data is collected, it would be easy to have two doors [relating to D17, where the initial consent mechanism idea was walking through the door]. But with more types of data it is difficult" (P10).

While text was mentioned as an easy and established tool to document relevant information (P5), especially long blocks of text can lead users who "just want to play the game [to] just accept because it is easier" (P5), which in turn would not result in informed consent. When a lot of information about the data collection is shared with users, the designers also mentioned the risk of "frightening the user" (P11) by bringing the privacy aspects to their attention in the first place.

Another aspect adding complexity is related to the information inferrable from the collected data. While this inferred information is often less obvious than the basic sensor data, it can reveal sensitive information (e.g., gender). Informed consent should include awareness of the consequences of data collection and also cover the inferred data (P9, P10).

Usability. Participants noted that the action to accept or decline data collection must be intuitive and accessible to users with disabilities (P5), for example, by not relying on hearing abilities or speech as the only option to interact with the privacy mechanisms. P8 also highlighted the need to communicate the current tracking state to the user so that they are aware of it at all times. In addition, designers highlighted limitations of current privacy mechanisms for 2D environments, including deceptive designs (P3), walls of text (P3, P8-9), lack of transparency (P2), and limited user-friendliness (P2, P8).

Aesthetics. Participants highlighted that a fitting aesthetic design of the privacy notice could help maintain the sense of presence in the VR environment. This can also be supported by using immersive game elements as an interaction method for the privacy decision (P2, P7, P9, P10) and by choosing a format that is appealing to the user (P10, P11) to prevent disrupting the VR experience.

Consent Interaction. Acquiring the user's explicit consent is critical. P5 highlighted the need for a fallback when users neither accept nor reject permissions, such as by ignoring the prompt. P8 proposed blocking other game elements until a decision is made, thus enforcing a response. In VR contexts, P5 underscored the importance of adapting consent interactions to each specific setting, with P6 arguing that general solutions are often insufficient and may require custom designs—albeit at a higher development cost. Finally, P5 questioned whether reducing text for a more immersive experience might reduce clarity, risking unintended user choices.

Technology Challenges. Due to the sensors used in XR devices, constant data collection is a key aspect (P10). Multiple participants (P2, P5-6, P9-11) stressed the importance of obtaining consent before the tracking begins. P5 and P6 discussed the importance of persistent privacy choices across multiple sessions to improve usability and prevent repetitive interactions. Another challenge arises when users want to revoke consent after initially agreeing to data collection. P5 mentioned a potential conflict if the data had already been shared with third parties or combined with other data points to infer further information about the user, making reversal difficult.

Alternative Game Elements. Several designers (P2, P5, P8-12) brought up the importance of alternative game elements to allow

users to continue using the application even if they do not (fully) consent to sharing their data. These elements should be easy to understand and ideally as playful as the original interaction (P8).

4.6.4 Properties of the Privacy Mechanisms. The categories identified within this theme are: *Information, Presentation, Control, Placement,* and *Timing*.

Information. Participants stressed that notices should specify which data types are collected (e.g., height, wingspan) and what can be inferred from them (e.g., gender), along with explaining why these data are needed. They also noted the importance of conveying the potential consequences of a user's privacy choices, including how interaction with the application might change. To manage the amount of information displayed, some suggested providing a link to a more detailed policy. Additionally, participants recommended offering an overview of collected data after consent, enabling users to review what has been captured.

Presentation. Participants discussed different ways to present privacy notices, such as the use of text (P5, P8) and symbols (P10). They emphasized the need to keep the amount of presented information manageable for the user (P10), adapt it to previous choices, and keep the interaction serious but fun to make it engaging while still fulfilling the purpose of a privacy control mechanism.

Control. Explicit user consent was seen as crucial by participants: "There needs to be the step of confirmation" (P11). Consent should be given through an *opt-in* mechanism rather than default collection. Control options should include reviewing collected data (P9), deleting it, and revocation of past decisions.

Placement. The designers explored different placement options for privacy notices, including integrating the notice with the VR environment and the existing game elements (P9). The notice should be reachable for the user (P4) to make it easy for them to interact with it. Most designs placed the notice in front or at the start of the room (P5, P10, P11), so either located where the user would enter (P11) or get teleported to, ensuring they face it directly and get prompted to interact (P9). Another idea was to position another part of the notice at the end of the room, informing users about the data collected during that section of the game: "At the end of the game (...) you can look at [your inventory] and see the data" (P10).

Timing. Beyond placement, designers suggested that certain actions could trigger the start of the interaction or present symbols to inform the user about which actions cause their data to be collected and when, for example, using "notification pop-ups that you got some new [data] entry" (P11).

5 Design Reiteration

After the brainstorming and sketching sessions, we reviewed all design concepts in Table 1 of type *Informed Consent*, i.e., the ones that propose both an awareness and a control mechanism. We excluded design D5, because its control mechanism required collecting user (telemetry) data. D2 and D4 were similar – representing consent through an embodied user interaction with a virtual piece of paper. We proceeded with D2 for further refinement. We re-sketched D2, D12, and D17 with added detail to ensure they accurately represented the proposed data collection awareness and control mechanisms. We provide a brief description of the refined concepts:

Sticker Book Accept and deny stickers are displayed at the door of each room for each type of data being collected (Figure 1A). The player exercises control by placing these stickers in their privacy book, which is part of their assets. This book allows players to manage and adjust their data permissions by adding or removing stickers, effectively accepting or denying data collection as needed.

Privacy Post The player is teleported into the room, facing a work desk. On the desk, a computer screen displays a privacy notice outlining the data that will be collected. They can sign it using the keyboard before using the printer next to the monitor to print the notice. Next to the desk, two pneumatic tubes are mounted on the wall: a green tube labeled "Yes" and a red tube labeled "No" (Figure 1B). To grant permission, the player inserts the printed notice into the green tube; to refuse, they place it in the red tube.

Consent Canvas The player is teleported in front of a whiteboard displaying information about the data that will be collected in the room (Figure 1C). The telemetry data, e.g., height and wingspan, is visually represented through a stick figure drawing. To accept or deny data collection, players interact with two erasers: a green eraser for acceptance and a red eraser for denial. If the player uses the red eraser to remove the information and, thus, denies data collection, an alternative way of solving the puzzle is triggered. Instead of physically performing the actions with their body, the player must draw the required poses on the whiteboard to uncover the codeword.

6 Focus Group

We conducted a focus group with usable privacy experts to evaluate the three reiterated designs and explore challenges and opportunities in developing usable privacy mechanisms for VR.

6.1 Procedure

The focus group was structured in two parts. After a brief introduction to the study's context and a presentation of the reiterated designs (*Sticker Book*, *Privacy Post*, and *Consent Canvas*), the first part involved a hands-on SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis [44] to better structure and prompt discussion. The experts first analyzed each design concept individually using the SWOT matrix, followed by a group discussion. Based on these discussions, the experts were asked to draft design recommendations for usable privacy mechanisms in VR on paper, which were then collectively discussed.

The second part of the session focused on broader challenges and trade-offs in designing privacy-aware data collection and control interfaces. We presented challenges identified during the earlier design sessions on separate post-it notes, which were thematically organized on a whiteboard. We then invited the experts to comment, reorganize, and add any aspects that might be missing from the overview, providing further recommendations specific to the challenges the novice game developers and designers faced. The

session concluded with a wrap-up and final comments. The focus group session lasted 90 minutes.

6.2 Participants

The focus group included four participants (3 males, 1 female), aged 24–31 (mean age 28.25, SD 2.68), recruited from the authors' academic research network. All focus group experts pursue or have completed a PhD in usable security and privacy. One of the experts (E3) also had 3 years of experience in XR research and development.

6.3 Data Analysis

We recorded approximately 90 minutes of audio, transcribed using MAXQDA transcription software. Using inductive thematic analysis [25], two researchers independently conducted open coding in MAXQDA, then met to discuss the initial codes and collaboratively developed a common codebook. The codes were analyzed and grouped into overarching themes. In addition, the individual SWOT matrices were compiled into a joint table to identify patterns and points of agreement/disagreement. These insights supported the interpretation of the qualitative data and are reflected in the reported results.

6.4 Results Focus Group

This section details the themes that emerged in the thematic analysis of the focus group session (see Figure 4).

6.4.1 Challenges. We identified four themes that addressed challenges and points to consider when creating privacy mechanisms for VR environments: *Practical Obstacles, Risks, Responsibility,* and *Trade-offs*.

Practical Obstacles. The experts identified two areas: user-related and designer/developer-related obstacles. From the user perspective, some users might not want to deal with privacy notices (E2). In combination with being unable to progress within the app without making a privacy choice, users might rush through notices without fully considering them, as mentioned by E4: "I do not think that you make people really carefully read the permissions". Additionally, with VR sensors collecting various types of data, privacy mechanisms must avoid simply replicating existing issues – "I do not want another Cookie Banner" (E1). Even with privacy mechanisms in place, user trust remains a challenge. Some users may doubt whether the software actually preserves privacy, preferring to rely on the OS to control sensor access: "I would only trust the OS to allow certain sensors to be accessed by the game" (E1).

From the developer's perspective, the experts acknowledged the high burden on developers (E1). They must balance user needs and preferences with company demands (E3). This can mean finding a solution that maintains presence during privacy interactions without compromising the gameplay experience. However, the privacy mechanism should not be too similar to the game mechanics, as this might spoil the experience ("have something similar, but not in the context of the game, not to spoil it" (E4)).

Risks. The experts identified several risks associated with VR privacy mechanisms. While some, like manipulating users by "hav[ing] hidden information in the text, like fine print" (E3) or purposefully designing mechanisms in a non-understandable way (E3), are common across digital platforms, others are unique to VR due to their immersive nature. Seamlessly integrated mechanisms might blur the line between VR and real-world implications of data collection: "In particular, in an immersive game, it might not be clear if this is in-game or out of the game" (E2). E2 argued that to avoid this, it might be necessary to "break the fourth wall" and thus the immersion. This goes along with the experts' concern that overgamification could cause users not to take privacy decisions seriously (E1). The experts also noted that alternative game elements – designed to avoid certain types of data collection – "might still reveal other data" (E2), which would need to be covered by privacy mechanisms. Finally, they raised concerns about how mechanisms would adapt to multiplayer scenarios, e.g., for social VR (E4).

Responsibility. A recurring discussion point was the question of responsibility. With multiple stakeholders involved, the experts discussed that the responsibility could lie with the app developers or device manufacturers. One perspective was that the OS should be the trusted party handling privacy mechanism: "I would only want certain privacy and sensor level based decisions to be asked once by the OS" (E1). Another perspective involved legal requirements (E1), which ideally would cover all necessary aspects (but would still leave the implementation with one of the other parties).

Trade-offs. The experts highlighted several trade-offs when designing privacy mechanisms, as not all aspects align. One key challenge is balancing complexity with comprehension and understandability: "How can I have a nice trade-off between complexity and comprehension for the user?" (E3). This trade-off also affects implementation: "If you want to make it granular for sensors, it is the easiest to implement, but the hardest to understand" (E2). Another concern was the point at which the user is overwhelmed or even frightened by the information provided which "is kind of in contrast to the transparency the company should give" (E3). The experts also discussed design trade-offs, such as whether to use global settings — to avoid overwhelming users with too many decisions, or local settings — to allow for granular privacy controls closely positioned to the corresponding game elements (E2). Another key balance is between making privacy interactions engaging and fun while ensuring they remain serious and effective as privacy mechanisms (E1).

6.4.2 Improvements. This section outlines design improvements suggested by the experts on the examples of the three design concepts, but they can also be applied to other designs.

Based on the discussion about the *Sticker Book*, several potential improvements were brought up: Instead of asking for the privacy decision at the door before the user enters the room, the experts suggested to *move the choice of stickers closer to the corresponding game interaction* so it would be clearer what would happen in the room, how the data would be collected, and how it would be used in the game context ("then it is more clear why it is used and what for" (E2)). Next, the experts discussed that the user should *be able to change their decision later*, which would mean that they can switch out the stickers anytime, "to have the opportunity also to change your mind after entering the room" (E4).

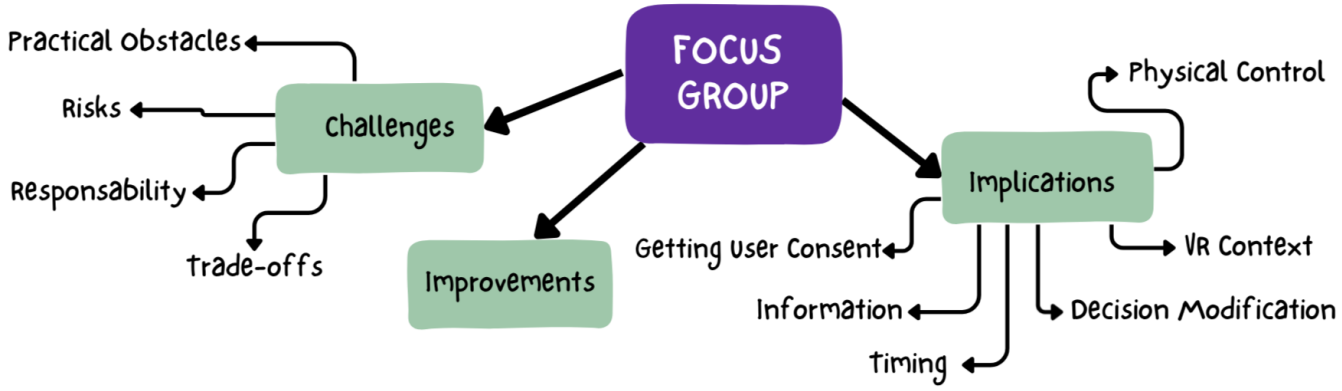

Figure 4: Overview of themes emerging from the thematic analysis of the focus group, with three main identified themes: Challenges, Improvements, and Implications.

The experts suggested to implement a *default setting to less data collection* for *Privacy Post*, in which initially only the green tube would be needed. In this way, only if the user wanted to give *explicit consent* to the data collection they had to do something (send the permission through the green tube) otherwise no action would be needed ("I just give active permission to the things I want to use. But I do not need to decline permissions" (E3)). Lastly, experts suggested that similar to the *Sticker Book*, *use of icons* could help to make the interaction more engaging (E2).

For *Consent Canvas*, the experts did not mention specific improvements, but their critique points also provided insight into how the design might be improved. Although they thought of the eraser as a fitting interaction mechanic to delete permission or collected data, using the green eraser to give consent seemed counterintuitive (E1), so the experts proposed choosing a more suitable interaction mechanism. To allow the user to *review their previously made decision*, they also suggested "take a picture [of the flip chart] or just document it somewhere" (E4) for future access.

6.4.3 Implications. We identified six code groups within this theme: *Getting User Consent, Information, Timing, Decision Modification, VR Context,* and *Physical Control.*

Getting User Consent. This was seen as the main purpose of the privacy mechanism. The experts mentioned important aspects of achieving this in a privacy-preserving way. Requiring the user to provide explicit consent was noted as a positive aspect of the designs several times: "I like that [the *Sticker Book*] forces people to interact. It makes the decision explicit" (E2). This closely relates to the privacy-by-design approach, including things such as "provid[ing] a privacy-preserving default" (E1), where permissions are declined unless the user actively opts in. Another key aspect is ensuring that permissions are tied to a specific purpose, with clear details provided in the privacy mechanism (E2). This can be reinforced by closely tying the privacy decision to the corresponding interaction through timing and placement (E2). Additionally, the privacy mechanism should allow for granular decisions instead of an all-or-nothing approach and reflect this in the design in a clear way (E4).

Information. To provide informed consent, a clear understanding on the user's side is needed. As already mentioned, the notice needs to contain information about the purpose of the data collection: "The main question is the purpose, so what is done with [the data]? " (E2); "make it clear what the consequences are for the participants if they allow or deny specific permissions" (E4). When designing immersive solutions, special attention is needed to avoid having immersive but unclear designs: If symbols are used, their meaning has to be clear and unambiguous (E4) to avoid confusion or even deceptive designs. In VR environments, where the collected data may vary depending on the user's position, it is "important to let the player always be aware of the state of tracking" (E3). This could be achieved by (visually) communicating an ongoing recording or notifying the user when a sensor is activated (E1).

Timing. The experts generally recommended placing the privacy mechanism at the start of the game (or room), though alternative approaches could be useful depending on the context. Using the timing to communicate which interaction belongs to which permission was mentioned as an effective way to leverage the VR environment to enhance the design of the privacy mechanisms: "One opportunity would be to tie this interaction not to a room, but to the interaction where the data is collected" (E2).

Decision Modification. Experts strongly recommended allowing users to review, revoke, and modify their privacy decisions after their initial choice. This includes providing access to previously collected data and the ability to delete it if consent is withdrawn: "You can change your mind, deny your permission, and then the recorded data will be deleted for that user" (E4).

VR Context. The experts proposed several recommendations to address VR-specific challenges while leveraging its immersive nature. One major aspect is gamification. While holding the risk of distracting the user from the original purpose of informing and providing control, it also has the potential to "keep it interactive and (...) make it more interesting" (E4), provided that appropriate design elements are used. Using gamification can make the privacy interaction engaging and thus increase the users' awareness and attention towards privacy.

To integrate the privacy decision into VR, using it as a tutorial for interaction methods was suggested: "It reminds me of tutorials (...), this is how you do it, and by the way, this is what you are revealing by doing it" (E2). To avoid spoiling too much of the game, the interaction context should be similar but still on an abstract level (E4). Other examples included short animations or interactive videos to clarify the meaning of symbols and icons (E4) and a "physical representation of your privacy decision" (E2) to make it more tangible for the user. While interactive elements within the privacy mechanism can be appealing, it is important that the "approach works well for different numbers of participants and different numbers of icons" (E4) and scales well with an increasing number of permissions. Also, the more closely related the collected data is to the game mechanics, the more important it is to provide alternative game elements alongside the privacy mechanism to "make the app or game usable, even without giving a single permission" (E3).

Physical Control. Experts noted that existing privacy mechanisms often depend on trust that the application genuinely deactivates denied sensors (E3). Implementing physical controls (e.g., unplugging sensors) removes this reliance, reassuring users that their choices are upheld. Alternatively, obfuscation techniques via middleware (e.g., using normalized data values (E2)) also protect privacy but shift trust to the middleware. These strategies enable users to continue using the application without disclosing all data.

7 Design Implications

Drawing on the design sessions and the expert focus group, we distilled a set of design implications for privacy interfaces in VR. They reflect both established usable privacy principles and novel insights that arise for HMD-based sensor-rich virtual environments.

7.1 Privacy-by-Design and Data Minimization in VR

Our findings underscore the importance of embedding privacy-by-design principles in VR, emphasizing minimal data collection and strong user control. Experts recommended *privacy-preserving defaults*, which limit data collection to what is essential for core functionality, and any additional collection requiring *explicit user consent*. They also advocate *purpose-tied consent mechanisms*, where consent applies only to the specific features or functionalities in question, rather than blanket permissions. These insights align with prior work [4] and GDPR requirements; however, the design sessions showed that many participants were unfamiliar with applying them in practice.

Implication 1: Use Explicit, Purpose-Tied Consent Mechanisms. Ensure that each data collection request is clearly tied to a specific purpose, with data collection set to the minimum necessary by default unless users actively opt in.

7.2 Granular Control and Transparency

Our results underscore the value of *granular control* over privacy settings, allowing users to specify exactly which data to share and adjust their choices later, including the ability to revoke consent or delete previously collected data. This flexibility gives users a sense of agency, but requires careful design to avoid overwhelming them with too many options. At the same time, transparency is essential to ensure that these choices are meaningful. *Continuous feedback*, such as ambient cues indicating active data collection, could help users stay aware of active data collection without breaking presence. Such cues are particularly crucial in VR, where full immersion may obscure real-time changes in collected data [31].

Implication 2: Provide Clear, Granular, and Modifiable Consent Options. Offer users detailed control options, prioritize critical settings to avoid overload, and enable them to revisit or revoke decisions at any time.

Implication 3: Enhance Transparency with Continuous Feedback. Provide real-time, context-sensitive feedback about ongoing data collection through persistent ambient indicators and just-in-time notifications, keeping users aware of when and why data is being collected while minimizing disruption to the immersive experience.

7.3 Gamification of Privacy Mechanisms

Designers and developers proposed using gamification elements, such as stickers and pneumatic mailing tubes, to incentivize users to engage in privacy decisions. These interactive elements hold particular value in VR contexts, where long text-based interfaces can suffer from poor readability [20]. Previous studies have explored gamified visualizations of collected data to improve the understandability of privacy policies [27, 30]. However, they focused on raising awareness rather than enabling control.

While integrating game mechanics into privacy interfaces can make privacy interactions more engaging [19], it poses the risk that users may not fully comprehend the implications of their choices, treating them as just another task to complete in the game rather than an important decision about their personal data. To mitigate this risk, it is important to *gamify privacy mechanisms thoughtfully*, ensuring that gamified interactions do not trivialize privacy choices or distract from critical information. Designers should carefully balance the engaging aspects of gamification with the need for clear communication of privacy risks and implications.

Implication 4: Gamify Privacy Mechanisms Thoughtfully. Incorporate gamification elements to engage users in making privacy decisions and increase usability in VR; ensure that gamified interactions do not trivialize privacy choices or distract from critical information about data collection.

8 User Evaluation

We applied the derived design implications to guide the implementation of a high-fidelity functional prototype of the *Sticker Book* interface and conducted an initial evaluation of its feasibility and user experience with end users. The *Sticker Book* was selected because it most closely reflected or allowed for key aspects of the

design implications: it supports explicit, purpose-tied consent, enables granular and modifiable permission choices, and employs clear interaction metaphors.

8.1 Study Procedure

In the user study, participants first provided informed consent and completed a demographics questionnaire to better contextualize their responses, including their prior VR experience and privacy attitudes as measured by the Internet Users' Information Privacy Concerns (IUIPC) scale [28]. Participants then completed a VR session in the adapted *MetaData* escape room [31], using the *Sticker Book* as a control interface for privacy permissions.

The session comprised six escape rooms, covering a range of different data types (body tracking, account information, eye tracking, location, voice recording, and cognitive performance). No actual participant data was collected; instead, the rooms presented plausible data requests only for the purpose of permission setting.

Data collection combined qualitative and quantitative measures. Quantitative data included the User Engagement Scale (UES) [34] and interaction logs. Qualitative insights were gathered through semi-structured interviews, with the interview protocol provided in Appendix B.

8.2 Apparatus

The *Sticker Book* was implemented using the Unity game engine[5] and evaluated on a Varjo VR-3 headset[6] paired with HTC Vive controllers. Users configured their privacy settings by dragging green (accept) or red (deny) stickers onto corresponding placeholders in a virtual book, each sticker representing a different data collection permission (Figure 5A). The book also included a short explanation of each data type and what it is used for in the game. Deny stickers were additionally visually distinguished with a strike-through icon. To support more efficient interaction, two additional bulk-decision buttons were added: "Accept All" and "Reject All". The implementation also included a persistent ambient indicator in the right upper corner signaling ongoing data collection (Figure 5B); and a contextual notification when users encountered a task requiring permissions they had not granted, prompting them to either skip the task or update their settings (Figure 5C).

8.3 Participants

Eighteen participants (8 female, 10 male) were recruited through university mailing lists and information channels. Seven were aged 18–24, ten were aged 25–34, and one was aged 35–44. Overall, participants reported relatively low prior VR experience, with a mean rating of $M = 3.17$ ($SD = 1.79$) on a 7-point Likert scale. In contrast, IUIPC scores indicated relatively high levels of privacy concern across all dimensions: awareness ($M = 6.31$, $SD = 0.38$), control ($M = 6.00$, $SD = 0.70$), and collection ($M = 5.88$, $SD = 0.49$). The study received ethics approval from LMU Munich (EK-MIS-2024-327). Each participant received €12 compensation and the study sessions lasted approximately 60 minutes.

[5]www.unity.com
[6]www.varjo.com

8.4 Limitations

The user study provides initial validation of the *Sticker Book* privacy interface with end users in VR; however, several limitations should be noted.

First, we implemented and evaluated only one of the design concepts. This allowed us to achieve high prototype fidelity and ecological validity, but it limits insights into alternative approaches. Future work could extend the evaluation to multiple design concepts for comparative analysis.

Second, the study was conducted within a single session. While this reduced participant burden and ensured focused assessment, it does not capture long-term use, habituation effects, or potential privacy fatigue. Longitudinal studies could provide deeper insight into how privacy-related interactions and decision-making in VR evolve over time.

Lastly, while comparative evaluation against conventional permission dialogs would be valuable, designing an appropriate baseline for embodied VR privacy interfaces is non-trivial. Existing permission prompts typically provide only binary, one-time consent and do not support several of the capabilities explored in this work, including granular permissions, permission revision, and contextual notifications. Consequently, such a comparison would risk conflating multiple design dimensions. Our exploratory evaluation therefore focused only on assessing the feasibility and user experience of the proposed interface. Future work could systematically isolate and investigate the contribution of individual design elements, such as gamification, contextual awareness cues, and granular control.

8.5 Results User Evaluation

In this section, we present the quantitative and qualitative findings from the exploratory evaluation of the *Sticker Book* prototype.

8.5.1 Quantitative Results. We report the quantitative results from the study, including user engagement and interaction logs.

User Engagement. User engagement was assessed using the UES across four dimensions: Perceived Usability, Aesthetic Appeal, Focused Attention, and Reward. Overall, the *Sticker Book* achieved a mean UES score of $M = 4.29$ ($SD = 0.34$), indicating a high level of user engagement.

Interaction Logs. Interaction log data showed that participants spent on average $M = 1.6$ min ($SD = 1.0$ min) interacting with the *Sticker Book*. Ten out of eighteen participants chose not to grant all permissions at the beginning of the session, most frequently denying location and voice data access. Of these participants, two participants opted to skip a room rather than grant location access; the remaining participants adjusted their permission settings in situ when prompted.

8.5.2 Qualitative Results. To better understand participants' experiences with the interface, we conducted a thematic analysis of the interview transcripts. We organized the qualitative findings into six themes: *Quality of Presentation*, *Impact on User Experience*, *Permission Reconsideration*, *Interface Preferences*, *Improvements*, and *Broader Reflections on Privacy*.

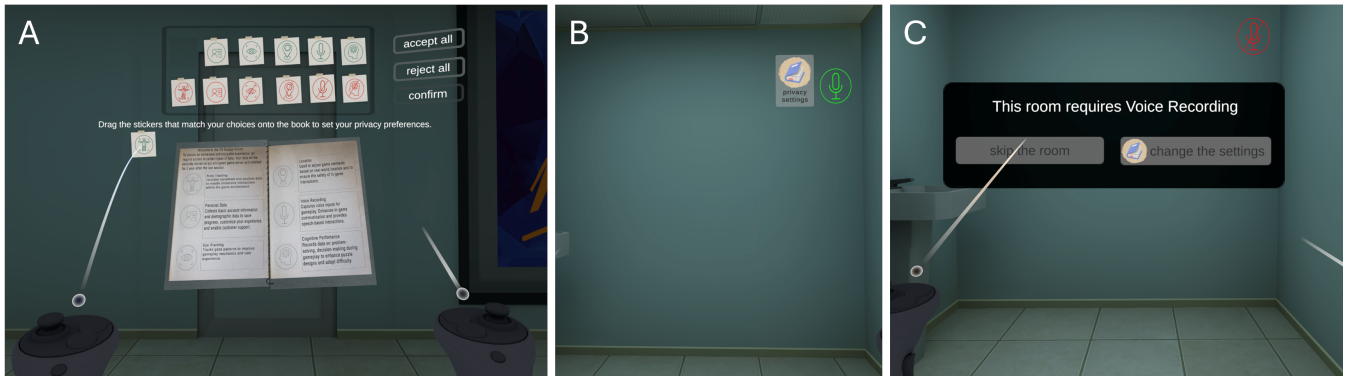

Figure 5: (A) The *Sticker Book* interface allows users to configure data collection preferences by placing accept or deny stickers into a virtual privacy book. (B) An ambient indicator in the upper right corner signals ongoing data collection. (C) A just-in-time notification appears when a task requires access to data (e.g., voice recording) for which the user has not granted permission, prompting either to skip the room or adjust the permission settings.

Quality of Presentation. Participants generally found the *Sticker Book* fun, eye-catching and effective in drawing attention to permissions: "you need to select the sticker and put it on the specific icon so that it drags your attention" (U4). The icons were described as intuitive, and memorable, helping to convey information with little text: "visual image in front of you, so you could see straight away what it was about...and also the little text underneath" (U12); "there was a lot less text and with symbols... I could choose what exactly I agreed to and what I didn't" (U5). However, some noted that certain information, such as conditions of data use, might get lost in the simplified visual form (U14).

Impact on User Experience. Participants generally reported a strong sense of control through granular choices and the ability to change their decision at any time with the *Sticker Book*: "I had the choice to choose which data I want to share" (U9); "I liked it actually that I can just change it anytime I want. Because in the usual ones you can't change it anymore" (U6). Some appreciated the active in-game data collection indicators: "there was this eye tracking icon and you could actually see that it was collected...it didn't get lost in the memory" (U8). Others appreciated the resulting sense of transparency: "it does feel like whoever is developing the game wants you to be able to make an informed choice" (U11).

However, several participants also reflected on the balance between privacy support and gameplay. While some felt that the additional privacy interactions slightly disrupted immersion: "it took you a little bit out of your immersive experience" (U15), others noted that making privacy more salient could even discourage continued engagement with the game: "it could be that I just stop playing the game because I've thought so much about what will happen to my data" (U18).

Permission Reconsideration. Interview responses provided insight into why some participants revised previously denied permissions during the experience, complementing the interaction log data. Some participants reported that contextual just-in-time requests clarified why a permission was required for a specific interaction: "I didn't agree to my voice and then I was in the exact room where they needed my voice...then I knew, ah, that's why they need it and I think that's good, that you know why it's needed in practice" (U5); "...you could really feel okay that's needed because of that specific feature" (U2). Others explained that they revised their permissions because they wanted to continue the experience rather than skip content, with one participant describing a "fear of missing out" (U11), while another reported: "I could have just skipped it, but because I really wanted to see it, I changed my mind" (U12).

Interface Preferences. Most participants (13/18) expressed a preference for the Sticker Book over a conventional "accept and continue" permission interface. Out of those, four participants preferred the *Sticker Book*, but proposed refinements, such as adding a full-text option (U12), simplifying the interaction (U5), being able to proceed with a meaningful alternative after initially denying a permission (U3), and tailoring the experience to individual privacy preferences (U9).

However, preferences were not universal and were sometimes influenced by user characteristics and usage context. One participant (U10) stated a preference for conventional privacy interfaces due to familiarity, but noted that "for kids, who are not really aware of data privacy, maybe the *Sticker Book* would be better." Another participant (U1) emphasized the importance of context, preferring conventional privacy interfaces at home, but the *Sticker Book* in public because of greater privacy concerns.

Improvements. Participants proposed several refinements to the *Sticker Book*. Suggestions included adding a full-text option (U12), providing more concrete explanations why particular data is needed, especially for reoccurring prompts (U2), what happens with the data afterwards (U16), as well as an early reminder "that you can change your settings anytime" (U13). While many liked the drag-and-drop interaction, some suggested: "click once to permit to click twice to deny on the sticker... just to speed it up. I mean, yes, it is more fun to drag it into the book... but if I imagine... a game like once a day... I would probably get tired of it rather quickly." (U14). Lastly, participants highlighted the need for data-minimizing alternatives that still allow gameplay without granting

full permissions: "that I can disagree and then still play the game, that would be perfect" (U18); "Can we still get things done without accepting certain terms?" (U3).

Broader Reflections on Privacy. This theme contains participant reflections on data privacy management, beyond the specific UI. Some noted that privacy decisions "depend on how important privacy is to you as a person" (U11), while others expressed resignation: "Nowadays... people don't care that much... people are not that aware of their rights and if there's a leakage then for regular people, there's not much they can do" (U3). Some also described erosion of choice: "we are no longer used to seeing and deciding what data we can share and what we cannot " (U17). U17 also argued that greater awareness of the collected data alone does not make them better protected, and U6 pointed out the lack of real alternatives when permissions are required to proceed.

9 Discussion

This section synthesizes findings across the participatory design sessions, expert focus group, and exploratory user evaluation, relating them to prior work and highlighting key challenges and implications for designing usable privacy interfaces in VR. While mixed-method approaches are well established in HCI, applying this end-to-end participatory design and evaluation process to VR privacy is, to our knowledge, novel. In addition to deriving design implications, we iteratively translated these into an interactive VR prototype and explored how granular permissions, contextual prompts, and ambient indicators are experienced by users within a functional VR application. This process surfaced a recurring tension across all three stages: *how to support meaningful engagement with privacy decisions without creating undue pressure to consent.*

9.1 From One-Time Consent to Contextual Privacy Decisions

Across all stages of the study, a consistent design direction emerged — moving away from privacy management as a one-time administrative task at the beginning of an application towards privacy mechanisms embedded throughout the user experience. The *Sticker Book* prototype reflects this design direction by combining granular, revisable permission controls with contextual prompts and ambient indicators. During the user evaluation, several participants reported that the in-context permission requests helped them better understand why specific permissions were needed for particular interactions. Complementing the contextual prompts, participants reported that the ambient indicators made ongoing data collection more noticeable and contributed to a greater sense of transparency without requiring explicit interaction. While prior work has shown that permission interfaces can improve users' understanding by explicitly linking data access to application functionality during permission configuration [1], our findings further suggest that revisiting these decisions in context, when the requested data becomes relevant, can support understanding throughout the experience.

At the same time, contextual privacy mechanisms introduce new design challenges. Some participants found repeated permission requests disruptive to presence and gameplay, while others expressed frustration at being asked to reconsider permissions they believed had already been configured. These observations highlight a recurring tension in privacy interface design between empowering users with contextual choice and preserving the flow of the primary interaction [10, 45, 47]. These findings suggest that embedding privacy decisions throughout the experience creates new opportunities to support transparency and informed decision-making, while introducing new trade-offs around interruption and immersion, and raising questions about how such interactions influence users' subsequent privacy choices.

9.2 Supporting Engagement Without Undue Pressure

While the user evaluation suggests that contextual privacy mechanisms can support users' understanding, sense of control, and engagement with privacy decisions, it also revealed that these mechanisms may influence subsequent privacy choices in more complex ways. Understanding when such influences support informed consent and when they become undue pressure represents an important challenge for immersive privacy interface design.

Interaction logs showed that eight out of ten participants who initially denied permissions later revised their choices. Interview responses suggest that these changes occurred for multiple reasons. For some participants, contextual explanations clarified why permissions were required for a particular interaction, leading them to reconsider earlier decisions. Others reported changing permissions because they wished to continue the experience rather than skip content, citing curiosity or a fear of missing out (FoMO) as motivating factors. This aligns with Westin and Chiasson's description of FoMO as a driver of *reluctant privacy behaviors*, where users accept data collection not because they are comfortable with it, but because they do not want to miss out on app functionality [54].

These findings highlight an important ethical tension: the same mechanisms that support users in actively engaging with privacy decisions may also create situations in which users feel encouraged to grant permissions they would otherwise decline. Similar concerns emerged during the focus group, where experts cautioned that rich interaction techniques and gamified privacy mechanisms should not become subtle forms of persuasion or dark patterns [12, 23]. Future work could therefore investigate in greater depth how contextual privacy interfaces in immersive virtual environments can support meaningful engagement with privacy decisions while preserving the voluntariness of consent. Possible directions include exploring different degrees of gamification, providing meaningful alternatives when permissions are denied, and developing safeguards against manipulative design practices.

9.3 Beyond Interface Design: Accessibility, Scalability, and Responsibility

Our findings further suggest that designing usable privacy interfaces in VR extends beyond interface design alone. Throughout the participatory design sessions and expert focus group, participants identified broader technical, organizational, and accessibility-related challenges that influence whether contextual privacy mechanisms can be implemented and deployed in practice.

Designers emphasized the need to support diverse abilities through multimodal cues (visual, auditory, haptic), noting that inaccessible privacy interfaces risk misinterpretation of privacy controls, unintended data disclosure, or disengagement. In VR, these challenges become particularly important given the combination of continuous high-frequency sensing, data inference, and inherently multimodal interaction, making simplicity and clarity essential.

Beyond accessibility, participants also highlighted the challenge of scaling privacy mechanisms as VR systems incorporate additional sensors, inferred attributes, and multi-user experiences. Supporting scenarios such as social VR introduces further complexity through bystander privacy and increasingly heterogeneous data flows, requiring interfaces that balance comprehensive privacy controls with usability.

In practice, the feasibility of such designs also depends on platform constraints: OS-level permission models and available APIs may not provide the required flexibility [5], while commercial incentives often prioritize functionality and monetization over user control [7, 51]. Consequently, translating many of the design implications identified in this work into practice will likely require support from platform providers and broader regulatory frameworks, in addition to interface designers and developers.

10 Conclusion

In this paper, we explored how informed consent can be supported in sensor-rich HMD-based virtual environments through the design of usable privacy interfaces. We adopted a mixed-methods, design-led approach, combining participatory design sessions with novice game designers and developers, a focus group with privacy experts, and the implementation and exploratory evaluation of a high-fidelity VR prototype. Through this process, we generated and refined a set of VR privacy interface concepts (including *Sticker Book*, *Privacy Post*, and *Consent Canvas*) and identified recurring design tensions.

Our findings show that designing VR privacy interfaces requires balancing several competing goals, including increasing transparency without disrupting presence, providing granular control without overwhelming users, and encouraging engagement without undermining the seriousness of privacy decisions. These tensions informed a set of design implications highlighting privacy-preserving defaults, granular and revisable consent options, continuous feedback, and thoughtful gamification. We operationalized these implications in a high-fidelity VR prototype and explored how users experience granular permissions, contextual consent prompts, and ambient transparency cues embedded within a VR application.

Across all three stages of this work, a consistent design direction emerged: moving beyond one-time front-loaded consent towards contextual privacy mechanisms that embed consent throughout the VR experience. At the same time, the exploratory user evaluation surfaced an important tension: promoting user engagement with privacy decisions and preserving the voluntariness of those decisions are not always aligned goals. This highlights the need for further research into how to support meaningful engagement with privacy decisions without creating undue pressure to consent.

This work contributes to HCI and usable privacy research by offering empirically grounded insights and actionable guidance for designing for informed privacy consent in sensor-rich immersive virtual environments.

Acknowledgments

This work has received funding from the German Research Foundation (DFG) under grant agreement no. 521584224. We would like to thank all members of the USEC research group at LMU Munich for providing valuable feedback throughout the different stages of this research project. We also extend our gratitude to all participants in the user studies.

References

[1] Melvin Abraham, Mark Mcgill, and Mohamed Khamis. 2024. What You Experience is What We Collect: User Experience Based Fine-Grained Permissions for Everyday Augmented Reality. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 772, 24 pages. doi:10.1145/3613904.3642668

[2] Melvin Abraham, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 30, 12 pages. doi:10.1145/3546155.3546691

[3] 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 *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (Baltimore, MD). USENIX Association, Berkeley, CA, USA, 427–442. https://www.usenix.org/conference/soups2018/presentation/adams

[4] Ann Cavoukian. 2009. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009), 2009.

[5] Kaiming Cheng, Mattea Sim, Tadayoshi Kohno, and Franziska Roesner. 2025. User Comprehension and Comfort with Eye-Tracking and Hand-Tracking Permissions in Augmented Reality. In *Proceedings of the 2025 Symposium on Usable Security and Privacy (USEC)* (San Diego, CA, USA). 15th Usable Security and Privacy Symposium (USEC), Internet Society, Reston, VA, USA. doi:10.14722/usec.2025.23005

[6] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* 52, 6, Article 110 (oct 2019), 37 pages. doi:10.1145/3359626

[7] Itay P. Fainmesser, Andrea Galeotti, and Ruslan Momot. 2023. Digital Privacy. *Management Science* 69, 6 (2023), 3157–3173. arXiv:https://doi.org/10.1287/mnsc.2022.4513 doi:10.1287/mnsc.2022.4513

[8] Florian M. Farke, David G. Balash, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, CA, USA, 483–500. https://www.usenix.org/conference/usenixsecurity21/presentation/farke

[9] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Exploring User-Centered Security Design for Usable Authentication Ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 694, 15 pages. doi:10.1145/3411764.3445164

[10] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. doi:10.1145/3411764.3445148

[11] Gonzalo Munilla Garrido, Vivek Nair, and Dawn Song. 2024. SoK: Data Privacy in Virtual Reality. *Proceedings on Privacy Enhancing Technologies* 2024 (2024), 21–40. Issue 1.

[12] Hilda Hadan, Lydia Choong, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. *ACM Comput. Surv.* 56, 10, Article 250 (May 2024), 25 pages. doi:10.1145/3659945

[13] 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 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 784, 24 pages. doi:10.1145/3613904.3642104

[14] Samory Houzangbe, Dimitri Masson, Sylvain Fleury, David Antonio Gómez Jáuregui, Jeremy Legardeur, Simon Richir, and Nadine Couture. 2022. Is virtual reality the solution? A comparison between 3D and 2D creative sketching tools in the early design process. *Frontiers in Virtual Reality* 3 (2022), 1–16. doi:10.3389/frvir.2022.958223

[15] Duha Ibdah, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. 2021. "Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies. *IEEE Access* 9 (2021), 166465–166487. doi:10.1109/ACCESS.2021.3130086

[16] Ismat Jarin, Yu Duan, Rahmadi Trimananda, Hao Cui, Salma Elmalaki, and Athina Markopoulou. 2024. BehaVR: User Identification Based on VR Sensor Data. arXiv:2308.07304 [cs.HC] https://arxiv.org/abs/2308.07304

[17] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. doi:10.1145/1572532.1572538

[18] Jennifer King, Airi Lampinen, and Alex Smolen. 2011. Privacy: is there an app for that?. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 12, 20 pages. doi:10.1145/2078827.2078843

[19] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[20] Tanja Kojić, Danish Ali, Robert Greinacher, Sebastian Möller, and Jan-Niklas Voigt-Antons. 2020. User Experience of Reading in Virtual Reality — Finding Values for Text Distance, Size and Contrast. In *2020 Twelfth International Conference on Quality of Multimedia Experience (QoMEX)* (Athlone, Ireland). IEEE, New York, NY, USA, 1–6. doi:10.1109/QoMEX48832.2020.9123091

[21] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (Seoul, Republic of Korea) *(FAccT '22)*. Association for Computing Machinery, New York, NY, USA, 508–520. doi:10.1145/3531146.3533116

[22] Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2014. Using Statistical Information to Communicate Android Permission Risks to Users. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, New York, NY, USA, 48–55. doi:10.1109/STAST.2014.15

[23] Veronika Krauß, Pejman Saeghe, Alexander Boden, Mohamed Khamis, Mark McGill, Jan Gugenheimer, and Michael Nebeling. 2024. What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. *ACM Trans. Comput.-Hum. Interact.* 31, 3, Article 32 (Aug. 2024), 39 pages. doi:10.1145/3660340

[24] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. 2023. Surveilling the gamers: Privacy impacts of the video game industry. *Entertainment Computing* 44 (2023), 100537. doi:10.1016/j.entcom.2022.100537

[25] Udo Kuckartz and Stefan Rädiker. 2019. *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video*. Springer International Publishing, Cham. doi:10.1007/978-3-030-15671-8

[26] Jee Hyun Lee, Eun Kyoung Yang, and Zhong Yuan Sun. 2019. Design Cognitive Actions Stimulating Creativity in the VR Design Environment. In *Proceedings of the 2019 Conference on Creativity and Cognition* (San Diego, CA, USA) *(C&C '19)*. Association for Computing Machinery, New York, NY, USA, 604–611. doi:10.1145/3325480.3326575

[27] Junsu Lim, Hyeonggeun Yun, Auejin Ham, and Sunjun Kim. 2022. Mine Yourself!: A Role-playing Privacy Tutorial in Virtual Reality Environment. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 375, 7 pages. doi:10.1145/3491101.3519773

[28] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[29] Nurul Momen, Sven Bock, and Lothar Fritsch. 2020. Accept - Maybe - Decline: Introducing Partial Consent for the Permission-based Access Control Model of Android. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies* (Barcelona, Spain) *(SACMAT '20)*. Association for Computing Machinery, New York, NY, USA, 71–80. doi:10.1145/3381991.3395603

[30] Alistair Morrison, Donald McMillan, and Matthew Chalmers. 2014. Improving consent in large scale mobile HCI through personalised representations of data. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational* (Helsinki, Finland) *(NordiCHI '14)*. Association for Computing Machinery, New York, NY, USA, 471–480. doi:10.1145/2639189.2639239

[31] Vivek Nair, Gonzalo Munilla Garrido, Dawn Song, and James O'Brien. 2023. Exploring the privacy risks of adversarial VR game design. *Proceedings on Privacy Enhancing Technologies* 2023 (2023), 238–256. Issue 4. doi:10.56553/popets-2023-0108

[32] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song. 2023. Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA). USENIX Association, Berkeley, CA, USA, 895–910. https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification

[33] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147. arXiv:https://doi.org/10.1080/1369118X.2018.1486870 doi:10.1080/1369118X.2018.1486870

[34] Heather L. O'Brien, Paul Cairns, and Mark Hall. 2018. A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies* 112 (2018), 28–39. doi:10.1016/j.ijhcs.2018.01.004

[35] Viktorija Paneva, Marvin Strauss, Verena Winterhalter, Stefan Schneegass, and Florian Alt. 2024. Privacy in the Metaverse:. *IEEE Pervasive Computing* 23, 3 (2024), 73–78. doi:10.1109/MPRV.2024.3432953

[36] Viktorija Paneva, Verena Winterhalter, Franziska Augustinowski, and Florian Alt. 2025. User Understanding of Privacy Permissions in Mobile Augmented Reality: Perceptions and Misconceptions. *Proc. ACM Hum.-Comput. Interact.* 9, 5, Article MHCI037 (Sept. 2025), 17 pages. doi:10.1145/3743738

[37] 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* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300340

[38] Sarah Prange, Pascal Knierim, Gabriel Knoll, Felix Dietz, Alexander De Luca, and Florian Alt. 2024. I do (not) need that Feature! – Understanding Users' Awareness and Control of Privacy Permissions on Android Smartphones. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (Philadelphia, PA). USENIX Association, Berkeley, CA, USA. https://www.usenix.net/conference/soups2024/presentation/prange

[39] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. doi:10.1145/3411764.3445067

[40] Shwetha Rajaram, Chen Chen, Franziska Roesner, and Michael Nebeling. 2023. Eliciting Security & Privacy-Informed Sharing Techniques for Multi-User Augmented Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 98, 17 pages. doi:10.1145/3544548.3581089

[41] Shwetha Rajaram, Franziska Roesner, and Michael Nebeling. 2023. Reframe: An Augmented Reality Storyboarding Tool for Character-Driven Analysis of Security & Privacy Concerns. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology* (San Francisco, CA, USA) *(UIST '23)*. Association for Computing Machinery, New York, NY, USA, Article 117, 15 pages. doi:10.1145/3586183.3606750

[42] Prashanth Rajivan and Jean Camp. 2016. Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (Denver, CO). USENIX Association, Berkeley, CA, USA, 1–7. https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/rajivan

[43] Derek Reilly, Mohamad Salimian, Bonnie MacKay, Niels Mathiasen, W. Keith Edwards, and Juliano Franz. 2014. SecSpace: prototyping usable privacy and security for mixed reality collaborative environments. In *Proceedings of the 2014 ACM SIGCHI Symposium on Engineering Interactive Computing Systems* (Rome, Italy) *(EICS '14)*. Association for Computing Machinery, New York, NY, USA, 273–282. doi:10.1145/2607023.2607039

[44] Albert Rizzo and Gerard Jounghyun Kim. 2005. A SWOT Analysis of the Field of Virtual Reality Rehabilitation and Therapy. *Presence* 14, 2 (2005), 119–146. doi:10.1162/1054746053967094

[45] John A Rothchild. 2017. Against notice and choice: The manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else). *Clev. St. L. Rev.* 66 (2017), 559.

[46] Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2019. Secure Multi-User Content Sharing for Augmented Reality Applications. In *28th USENIX Security Symposium (USENIX Security 19)* (Santa Clara, CA, USA). USENIX Association, Berkeley, CA, USA, 141–158. https://www.usenix.org/conference/usenixsecurity19/presentation/ruth

[47] Robert H Sloan and Richard Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L.* 14 (2014), 370.

[48] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-Aware Eye Tracking Using Differential Privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications* (Denver, Colorado)

(ETRA '19). Association for Computing Machinery, New York, NY, USA, Article 27, 9 pages. doi:10.1145/3314111.3319915

[49] Luma Tabbaa, Ryan Searle, Saber Mirzaee Bafti, Md Moinul Hossain, Jittrapol Intarasisrisawat, Maxine Glancy, and Chee Siang Ang. 2022. VREED: Virtual Reality Emotion Recognition Dataset Using Eye Tracking & Physiological Measures. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 178 (Dec. 2022), 20 pages. doi:10.1145/3495002

[50] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 168, 24 pages. doi:10.1145/3544548.3581060

[51] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. 2022. OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR. In *31st USENIX Security Symposium (USENIX Security 22)* (Boston, MA). USENIX Association, Berkeley, CA, USA, 3789–3806. https://www.usenix.org/conference/usenixsecurity22/presentation/trimananda

[52] Vera Volk, Sarah Prange, and Florian Alt. 2022. PriCheck– An Online Privacy Assistant for Smart Device Purchases. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 275, 5 pages. doi:10.1145/3491101.3519827

[53] Hanqiu Wang, Zihao Zhan, Haoqi Shan, Siqi Dai, Maximilian Panoff, and Shuo Wang. 2024. GAZEploit: Remote Keystroke Inference Attack by Gaze Estimation from Avatar Views in VR/MR Devices. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1731–1745. doi:10.1145/3658644.3690285

[54] Fiona Westin and Sonia Chiasson. 2020. Opt out of privacy or "go home": understanding reluctant privacy behaviours through the FoMO-centric design paradigm. In *Proceedings of the New Security Paradigms Workshop* (San Carlos, Costa Rica) *(NSPW '19)*. Association for Computing Machinery, New York, NY, USA, 57–67. doi:10.1145/3368860.3368865

[55] Yuxia Zhan, Yan Meng, Lu Zhou, Yichang Xiong, Xiaokuan Zhang, Lichuan Ma, Guoxing Chen, Qingqi Pei, and Haojin Zhu. 2024. VPVet: Vetting Privacy Policies of Virtual Reality Apps. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1746–1760. doi:10.1145/3658644.3690321

A VR Environments (Concept Brainstorming and Sketching Sessions)

Figure 6: Puzzle rooms from the escape room game *MetaData* [31]. (A) The monitors display different letters on Ishihara color test plates. Depending on the word the user can read, color blindness can be inferred. (B) The user has to mimic the poses displayed on the wall to reveal the password, enabling measurement of their wingspan. (C) When the panels on the wall turn from red to green, the user has to press the button on the table to uncover the letter of the password, revealing their reaction time. (D) The password is written in different foreign languages around the room; the direction of the user's gaze reveals which language(s) they recognize.

B Interview Protocol (User Evaluation)

The following semi-structured interview protocol was used in the user evaluation of the *Sticker Book* interface. They were designed to capture user reflections on usability, understanding, perceived privacy protection, and overall experience.

(1) **Overall Experience**: Describe your experience with the *Sticker Book* privacy interface in your own words.
(2) **Perceived Strengths and Weaknesses**: What aspects of the interface did you like, and what aspects did you dislike?
(3) **Understanding of Permissions**: How well did you understand the permission controls?
(4) **Perceived Privacy Protection**: To what extent did you feel that the permission controls were sufficient to protect your privacy while using the application?
(5) **Suggestions for Improvement**: If you could change anything about the *Sticker Book* privacy interface, what would it be?
(6) **Interface Preference**: Which privacy interface would you prefer to use in VR applications: the *Sticker Book* or a conventional privacy permission interface (e.g., "accept and continue" permission prompts)?
(7) **Final Reflections**: Do you have any final thoughts or opinions you want to share about your experience?