Designing Effective Consent Mechanisms for Spontaneous Interactions in Augmented Reality

Maximiliane Windl
LMU Munich
Munich, Germany
Munich Center for Machine Learning (MCML)
Munich, Germany
maximiliane.windl@ifi.lmu.de

Petra Zsofia Laboda
LMU Munich
Munich, Germany
labodapetra@gmail.com

Sven Mayer
LMU Munich
Munich, Germany
info@sven-mayer.com

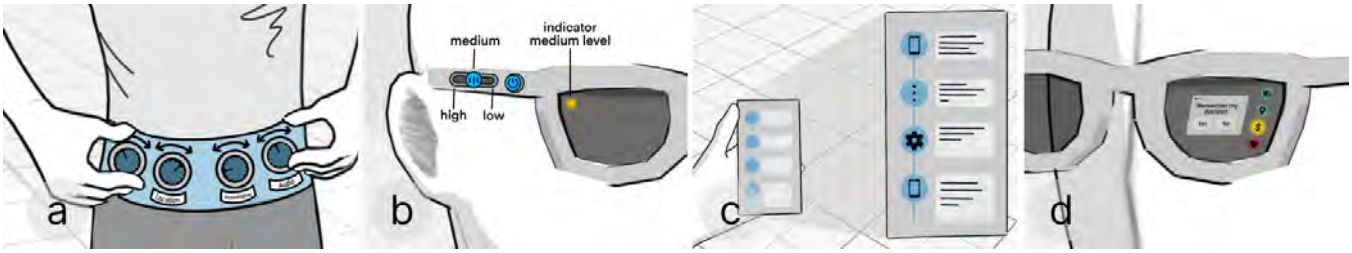

Figure 1: Expert interviewees suggested consent mechanisms for spontaneous AR interactions: a) a privacy belt; b) privacy sliders and buttons; c) a companion device to retrieve a privacy dashboard; d) data icons in the user's field of view.

Abstract

Ubiquitous computing devices like Augmented Reality (AR) glasses allow countless spontaneous interactions – all serving different goals. AR devices rely on data transfer to personalize recommendations and adapt to the user. Today's consent mechanisms, such as privacy policies, are suitable for long-lasting interactions; however, how users can consent to fast, spontaneous interactions is unclear. We first conducted two focus groups (N=17) to identify privacy-relevant scenarios in AR. We then conducted expert interviews (N=11) with co-design activities to establish effective consent mechanisms. Based on that, we contribute (1) a validated scenario taxonomy to define privacy-relevant AR interaction scenarios, (2) a flowchart to decide on the type of mechanisms considering contextual factors, (3) a design continuum and design aspects chart to create the mechanisms, and (4) a trade-off and prediction chart to evaluate the mechanism. Thus, we contribute a conceptual framework fostering a privacy-preserving future with AR.

CCS Concepts

• **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → **Human computer interaction (HCI)**.

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713519

Keywords

human-computer interaction, privacy, consent, augmented reality

ACM Reference Format:
Maximiliane Windl, Petra Zsofia Laboda, and Sven Mayer. 2025. Designing Effective Consent Mechanisms for Spontaneous Interactions in Augmented Reality. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3706598.3713519

1 Introduction

Researchers and lawmakers have long focused on communicating privacy information as they recognize the need to protect users when sensitive data gets processed and stored. Until today, disclosing comprehensive privacy information is still primarily done through privacy policies, even though research agrees that they lack effectiveness [31, 32, 36, 38]. One of their biggest problems is their length [16, 31, 36] and already today, users are reluctant to invest this time [36]. Thus, for cases where the interactions only take a split second, such as checking the heart rate or weather on a smartwatch, users are certainly unwilling to read a multi-page policy. Spontaneous interactions are characterized by a particularly short interaction duration and frequent repetitions. Here, the time to engage with the privacy information would easily exceed the interaction time. In addition, most ubiquitous devices would require a second device to access this textual privacy information, reinforcing another privacy policy problem – the missing but required link between the text and the interaction. Yet, context is one key factor in making privacy information more understandable [54].

This problem is expected to worsen as AR glasses become widely adopted. AR glasses will stimulate thousands of spontaneous interactions per day. As they are equipped with microphones and cameras, they greatly threaten users' privacy, often remaining "always on" while pointing toward people without requiring affirmative activation. This passive, continuous data collection heightens privacy concerns, as AR interactions are far more contextually embedded than traditional devices. Privacy concerns surrounding AR devices date back to models like Google Glass [17]. Today, with newer models such as Ray-Ban Meta smart glasses and portable XR devices like the Oculus Quest and Apple Vision Pro, these issues are becoming increasingly relevant as AR blends seamlessly into daily life. Prior work identified privacy concerns in AR, such as the extensive and continuous data collection [15], which systems can combine to infer more sensitive information [3, 8, 29]. Researchers have developed various consent mechanisms to address these issues. These include mechanisms where users actively grant or deny consent for data collection [25, 48] and systems that rely on user-defined preferences to determine appropriate data collection [30, 52]. Yet, it is unclear which mechanisms are most effective. Moreover, we lack an encompassing understanding of which mechanisms fulfill the unique requirements of *spontaneous* AR interaction scenarios, i.e., are quick and require little user effort while ensuring effective data protection.

This work investigates how effective privacy consent for spontaneous AR interactions can be realized. We first conducted two focus groups (N=17) to understand when and how spontaneous interaction scenarios with AR glasses leverage private information. Based on these findings, we constructed a scenario taxonomy. We then conducted in-depth interviews and co-design activities with privacy experts (N=11) to validate the taxonomy and establish effective consent mechanisms. Through these studies, we gained an understanding of privacy-relevant spontaneous interaction scenarios and the specific properties that determine the suitability of consent mechanisms. Based on our insights, we constructed a four-step framework that enables the design of effective consent mechanisms for such interactions.

This work makes the following key contributions. We provide (1) a validated scenario taxonomy to understand privacy-relevant AR interaction scenarios, (2) a flowchart to decide on the type of consent mechanisms while taking into account a situation's contextual factors, (3) a design continuum and design aspects chart to design and optimize the mechanisms, and (4) a trade-off panel and prediction chart to evaluate the mechanism in terms of (expected) user effort and comfort. Together, the tools form a framework for designing effective consent mechanisms for spontaneous AR interaction scenarios. The tools are designed to fit into the four phases of the User-Centered Design (UCD) process.

2 Related Work

We first present prior work on privacy concerns in AR and control mechanisms to mitigate these concerns. We then summarize prior work and point out the research gap we address with this paper.

2.1 AR Privacy Concerns

Prior research highlights that continuous recordings via AR glasses pose significant surveillance challenges [29, 43, 44]. These recordings extend beyond the primary user to include the physical environment and bystanders [10, 44]. Reflective surfaces of virtual objects further amplify privacy risks by exposing sensitive information from the real world, such as driver's licenses or credit cards [56]. Additionally, Roesner et al. [43] identified legal issues, including the unintentional capture of copyrighted material, which may violate intellectual property rights [43].

By investigating concerns about data types exceeding the contemporary technological capabilities of AR glasses, Gallardo et al. [15] found that users considered the collection of location, body temperature, heart rate, and movement acceptable, probably because they represent familiar practices from devices like smartphones and smartwatches [15]. In contrast, participants were uncomfortable with the collection of private conversations or activities, brain wave data and associated visual information, and employers monitoring employees. By combining data, it is possible to reveal even more private information. For example, researchers showed that combining video and audio content with biometric and character-specific attributes can enable conclusions about the individual [15]. Moreover, conversations can reveal relationships, and the specific conversation content can even impose social or legal consequences [15]. By associating visual information with time and location, researchers demonstrated that it is possible to determine preferences and habits [3, 8, 29]. Combining biometric data, voiceprints, and facial images facilitates identifying people in digital and physical environments [15]. In this context, the ability of AR technology to interpret facial expressions, gestures, and voice and monitor combined with biometric data, can reveal emotional states, thoughts, and feelings [3, 29]. Moreover, psychological and physiological data derived from biometric data enables predicting behavioral patterns [29], which can then be used to compile profiles of individuals [8]. Gallardo et al. [15] examined users' attitudes toward secondary usage of their information in the context of speculative consumer-grade AR glasses and found that users are skeptical toward the glasses' companies, employers, healthcare data recipients, insurance providers, and advertisers.

Research also identified contextual factors that impact privacy concerns, such as the location. While users considered using AR in private areas such as bathrooms or bedrooms too intimate and socially unacceptable, they were more comfortable in public spaces [12, 15]. Chung et al. [5] explained that in public environments such as professional meetings or classrooms, users expect appropriate behavior from other parties and associate it with fewer privacy incidents. Furthermore, consumers were more likely to accept AR glasses if they perceived them as a work-related tool [26]. People's relationships were another crucial factor in terms of technology acceptance [12]: There is a bond of trust with family members or friends, even if they wear AR glasses [5]. However, with strangers, the secondary users must understand the intentions of the person interacting to feel comfortable [5]. Similarly, Denning et al. [12] explained that bystanders' acceptance of AR recordings depends on what they are doing, how they behave at the moment of recording,

and the context of the future data release. Here, transparency reduces privacy concerns, as it is crucial for users to understand the device owner's monitoring and data processing actions [26]. Moreover, Gallardo et al. [15] suggested that the higher the emotional attachment to the device user, the more they avoid collecting sensitive data. Finally, Profita et al. [39] and Ahmed et al. [2] found that people generally accept assistive AR technologies, particularly in scenarios where fundamental demographic information or visually perceptible details are shared with people with visual impairments.

2.2 Privacy Control Mechanisms for AR

Previous research has introduced various control mechanisms to address privacy concerns. For example, Rajaram et al. [40] developed a storyboarding tool to help designers identify and mitigate privacy and security violations during the early stages of AR application development. This tool supports the exploration of mitigation strategies and interaction techniques to prevent privacy violations.

Researchers have also introduced various concrete mechanisms, many of which rely on active user involvement. For instance, Jana et al. [20] proposed a protection mechanism that enables users to monitor information flows and actively grant or revoke permissions as needed. Hu et al. [19] introduced *MagicCloth*, a cloth with a unique pattern to overlay privacy-sensitive objects indoors. When users cover items with it, the object gets replaced with virtual content adapted to its shape and size [19]. Further, the *Markit Framework* regulates the recording of sensitive information and objects in the environment through defined symbols and gestures [41]. Users can draw a rectangle around the information they want to protect, which then gets masked in real time. Roesner et al. [45] experimented with world-based access control, permitting objects, spaces, and individuals within the real world to communicate explicit guidelines through privacy passports [45]. An example is a privacy passport attached to a changing room that forbids video and audio recording: after scanning the pass, the camera and microphone get deactivated [45]. To address reflection-based privacy violations, Zhao et al. [56] developed mechanisms that modify the surface properties of reflective objects, for example, by increasing surface roughness. Other studies have explored the use of gestures or wearable tags to facilitate opt-in or opt-out decisions for data collection [25, 49]. While establishing representative gestures for these processes appears feasible, their practical implementation is hindered by ambiguity and the risk of misinterpretation [25].

Other mechanisms require less user involvement and implement privacy decisions (semi-)automatically. *PlaceAvoider* [52] allows users to define sensitive environments, such as bathrooms, where data collection is prohibited. It analyzes captured images, categorizes their content, and enforces user-defined preferences by blocking the release of prohibited data. Jana et al. [21] introduced *Darkly*, a protection layer that safeguards sensor data by converting it into abstract formats, preventing access by untrusted third-party applications. Similarly, *PrivacyManager* considers contextual factors, such as location, to restrict functionalities when it detects violations of predefined configurations [30]. Jensen et al. [22] and Hu et al. [18] disconnected the collection of camera images on the device from internet communication and denied uploading sensitive information to the network without user consent. In this context, Hu et al. [18] provided users with an interface to review data exchanges to actively control which visual data can enter the web. *Cardea* allowed users to apply privacy profiles to identify sensitive contextual factors of interactions and prohibit their recording [48]. As a further functionality of *Cardea*, bystanders can accept and reject real-time AR monitoring through gestures, whereby a refusal initiates the system to blur their faces [48]. Similarly, *BystandAR* [9] used eye and voice tracking to recognize the presence of bystanders and employ facial masking [9]. Alternatively, Ye et al. [55] developed negative face blurring, where users can train the system to identify specified faces as familiar identities and blur unfamiliar profiles. *Erebus* enables developers to translate fine-grained rules for sensor data into app-specific behavior policies [24]. It also provides users with customization options to modify predefined authorizations.

2.3 Summary and Research Gap

Prior work has highlighted various privacy concerns users face in AR environments, including the extensive data collection [15], which can be combined to infer private information [3, 8, 15, 29]. Additionally, studies have identified contextual factors that influence concerns [5, 12, 26]. Prior work created control mechanisms to mitigate these concerns, including gestures to allow or deny data collection [25, 48], methods to mark physical objects to prevent their recording in AR [19, 41], preference-based approaches that let users designate areas or information to remain private [30, 48, 52], and algorithms to obscure or abstract sensor data [9, 21, 55]. Yet, which mechanisms are most effective and best suited for specific situations is unclear. Moreover, as AR devices blend into daily life, interactions will become ubiquitous and seamless. Yet, what characteristics consent mechanisms must fulfill to satisfy the requirements of such *spontaneous interactions* is also unclear. This paper investigates how effective privacy consent for spontaneous AR interactions can be realized through the following two research questions. **RQ1**: How and under what conditions do spontaneous AR interactions leverage private information? **RQ2**: How can privacy consent mechanisms be designed to be effective and suitable for spontaneous, seamless interactions in everyday AR environments?

3 Understanding Privacy-Relevant AR Scenarios

We first aim to understand when and how spontaneous interactions leverage private information **(RQ1)**. Therefore, we conducted two focus groups with a total of 17 participants to understand the characteristics of spontaneous AR interaction scenarios. We provide the full focus group study guideline in the supplemental material. We obtained ethics approval in accordance with our local regulations.

3.1 Participants

As we aimed to recruit participants with prior AR experience, different cultural backgrounds, and expertise, we used a pre-screening questionnaire, see Appendix Section A.1.3. We distributed the questionnaire and respective study call over the university's mailing list[1]. Of the 17 participants (6 men and 11 women), most had used AR 1-3 times ($N = 8$), 5 had used it 4-7 times, two more than 7

[1]Mails sent over the mailing list go out to all university employees and affiliates, ranging from facility managers to professors.

times, and only two never before. Their ages ranged from 21 to 41 years ($M = 26$, $SD = 5.74$). A detailed overview of participants' demographics and expertise is presented in Table 1.

3.2 Procedure

We conducted two separate focus groups (see Table 1) on different days in one of our institution's meeting rooms. The same researcher conducted both sessions in English. After welcoming the participants, we asked them to complete an informed consent form and a demographic questionnaire. The sessions began with brief introductions, followed by an initial discussion of participants' experiences with AR, where they shared their prior exposure to the technology and their general attitudes toward it. We then familiarized the participants with the focus group's context through a presentation. For this, we painted a picture of a hypothetical future with AR, where people use AR glasses every day. We also defined spontaneous interactions with specific examples (see Appendix Section A.1.1) and familiarized the participants with the sensing capabilities of AR glasses (see Appendix Section A.1.2). Through this, we wanted to motivate participants to consider a broad spectrum of possibilities instead of limiting themselves to cameras and microphones.

In both focus groups (see Table 1), we grouped participants into pairs (with one group of three in Focus Group 1 due to an uneven number of participants) to discuss their views on data management in AR interaction scenarios. We encouraged them to broaden the discussion to include privacy-sensitive, emerging, and speculative data types, data actors (i.e., third parties involved in collecting, receiving, processing, or transferring user data [15]), and different target entities for data collection (e.g., primary users, bystanders, or secondary users). After they shared their insights, we introduced our curated list of privacy-sensitive data types, including speculative examples such as brainwave measurements (see Section 8).

To introduce the focus groups' speculative creation process, we contrasted an example of a car rental process, once using a standard smartphone and once using hypothetical AR glasses. We stressed that automated processes entail enhanced data gathering and processing, increasing the risk of data misuse. Then, we invited the participants to create interaction scenarios by describing a user journey. Here, we randomly assigned each pair to one of the following contexts to generate diverse examples: *(A) Travel and Transportation*, *(B) Retail and Shopping*, *(C) Healthcare and Wellness*, *(D) Education and Learning*, *(E) Home and Living*, *(F) Work and Productivity*, *(G) Entertainment and Leisure*, *(H) Social Interactions*, *(J) Safety and Security*, and *(K) Environmental and Sustainability*. We handed them a template, where they had to define the user's goal, describe the interaction steps, and list all personal data the AR glasses captured.

After the teams presented their scenarios, we analyzed each from a data protection perspective and explored their potential impact on everyday life. We concluded by compensating them with €20 for attending the two-hour session.

3.3 Data Analysis

We recorded 124 minutes of audio data in the first and 122 minutes in the second focus group. We transcribed the focus groups using a locally hosted instance of Whisper[2] and performed Thematic Analysis [4] using Atlas.ti (v. 24.1.1). First, two researchers independently coded 20% of the data. We then met to discuss the preliminary codes, clarify ambiguities, and define an initial codebook. Afterward, we divided the remaining statements among two researchers for coding. A third researcher joined in the final iteration round to identify code groups. We repeatedly discussed and revised all themes by comparing the coded segments across the groups. We provide the codebook as supplementary material.

3.4 Results: AR Interaction Scenarios

We identified three key aspects of AR interaction scenarios: (1) the purpose for which users engage with the device (*User Needs*), (2) the methods by which data is transferred (*Data Transfer*), and (3) the types of data being utilized (*Personal Data*). These aspects are consolidated into the scenario taxonomy (see Figure 2), which serves as a framework for defining privacy-relevant AR interaction scenarios. Each scenario begins with a context in which users employ AR glasses to address one or more *User Needs*. To fulfill these needs, the device performs *Data Transfers*, often repetitive in nature, resulting in extensive *Personal Data* usage throughout the scenario.

3.4.1 User Needs. We identified ten user needs. The first is *Assistance in Decision-Making*. Here, AR glasses present users with personal recommendations based on situational factors so that *"it's easier for [the users] to decide what [service or product] [they] want to choose"* (P15). *Augmented Perception* describes augmentations to expand their perception of the environment. Participants cited examples of movie theater or concert visits, where visual and auditory stimuli could get suppressed so that the visitor has the feeling of being *"alone in the concert for one song"* (P14). *Automation of Everyday Tasks* describes situations where AR glasses automate routines and administrative processes. Participants discussed automated ordering and purchasing processes (P2 - P4, P6, P7, P11, P12, P14, P15) or the automatic creation of personal calendar events (P1, P5 - P7, P11, P12, P17). *Health Monitoring and Treatment Management* describes situations where AR glasses help to control health metrics. For example, they assist in selecting food items (P8, P12) or record conversations at the doctor's office (P1). *Control of Connected Devices* refers to using AR glasses to interact with and control networked systems, automating tasks such as connecting AR glasses to smart home devices to assist with activities like cooking (P2). *Learning Support and Enhanced Effectiveness* refers to scenarios where AR glasses assist users in acquiring new skills or improving task performance. For example, they can display augmented overlays with step-by-step instructions for tasks like first aid (P13) or cooking (P2). Additionally, AR glasses can modify the visual environment to enhance focus or alleviate stress (P3). *Improvement of Communication* refers to the use of AR glasses to bridge communication gaps in everyday interactions, such as facilitating conversations with deaf or hard of hearing individuals (P12, P13) or recognizing gestures and facial expressions to bridge cultural differences (P13). *Intuitive Navigation* encompasses scenarios where users are guided to specific locations in real-time through overlay markers (P1, P5, P7, P11, P12, P14, P15). *Rapid Identification Procedures* describe the need for

[2] https://openai.com/index/whisper/

Table 1: Focus group participants' demographics: their country of birth, age, gender, education, profession, and AR experience.

	PID	Birth Country	Age	Gender	Education	Occupation	AR Experience
Focus Group 1	P1	Russia	23	Female	B.A. Sociology with Political Science	Student	1-3 times
	P2	China	25	Male	M.Sc. Epidemiology	Student	4-7 times
	P3	Germany	29	Male	M.Sc. Computer Science	Student	No experience
	P4	Germany	41	Male	LL.B. Law	Student	1-3 times
	P5	Russia	24	Female	B.A. Sociology with Computer Science	Student	1-3 times
	P6	USA	25	Female	M.Sc. Human-Computer Interaction	Student	4-7 times
	P7	Germany	23	Female	M.Sc. Human-Computer Interaction	Student	No experience
	P8	Germany	26	Female	M.Sc. Computer Science	Student	4-7 times
	P9	Turkey	25	Female	M.Sc. Computer Science	Student	7+ times
Focus Group 2	P10	Germany	24	Female	M.Sc. Human-Computer Interaction	Student	7+ times
	P11	Germany	24	Male	M.Sc. Human-Computer Interaction	Student	4-7 times
	P12	Italy	23	Male	M.Sc. Statistics	Student	4-7 times
	P13	Germany	23	Female	M.Sc. Computer Science	Student	1-3 times
	P14	Germany	22	Male	M.Sc. Computer Science	Student	1-3 times
	P15	Germany	23	Female	M.Sc. Human Factors Engineering	Student	1-3 times
	P16	Australia	41	Female	M.A. Cultural Anthropology	Office Manager	1-3 times
	P17	Bulgaria	21	Female	B.Sc. Psychology	Student	1-3 times

automated authentication processes, for instance, to grant quicker admission to events or access to buildings (P7). Finally, *Rapid Information Access and Retrieval* involves the use of AR to provide direct and selective information displays within the user's field of view (P1 - P8, P10, P12 - P17).

3.4.2 Data Transfer. We identified data transfer stages by systematically analyzing interaction patterns that describe how data is recorded, processed, and transferred to external systems or devices. *Data Collection* refers to the initial recording of data, such as biometric identifiers (P7, P11, P15), location data (P5, P6, P7, P11, P15), or physiological measurements (P3, P14, P15). The second stage, *Data Processing*, involves operations performed on the recorded data, such as object identification (P10), gesture interpretation (P7, P13), or generating a navigation map from location data (P11, P15). Finally, *Data Transfer* refers to transmitting personal information to external services or devices, playing a critical role in tasks like payment or booking procedures (P2, P5, P7, P11). These three stages build on one another, forming a sequence in data management for AR applications. However, some scenarios omit the *Data Transfer* stage when the recorded data remains on the user's device.

3.4.3 Personal Data. Our participants identified 20 categories of personal data types, as shown in Figure 2. Some of these data types are interrelated; for instance, visual recordings can also capture location or activity data. *Personal Characteristics* include attributes such as gender identity, age, or sexuality, a term we adopted from O'Hagan et al. [37]. *Outdoor/Indoor Spaces* refers to environmental data, such as private or public spaces the user visits. *Disorders* can be detected through physiological data (P3) or revealed during medical consultations (P1, P2). Lastly, *Personal Developments* covers activities and data related to skill-building and human capital, such as users' learning progress (P3, P4, P10, P11).

Table 2: The detailed demographics of the experts. Residency (Res.) abbreviations according to ISO 3166-1.

EID	Age	Gen.	Res.	Birth	Edu.	Exp.	Sector
E1	29	M	DEU	Europe	M. Sc.	3y	Academia
E2	34	M	DEU	Europe	Ph.D.	4y	Academia
E3	37	M	CAN	Europe	Ph.D.	8y	Industry
E4	28	M	DEU	Europe	M. Sc.	1y	Academia
E5	29	M	DEU	Europe	M. Sc.	3y	Academia
E6	29	M	CHE	Europe	Ph.D.	5y	Academia
E7	27	F	DEU	Europe	M. Sc.	1y	Academia
E8	27	M	DEU	Europe	M. Sc.	1.5y	Academia
E9	36	F	DEU	Africa	Ph.D.	4y	Academia
E10	33	M	DEU	Asia	Ph.D.	5y	Academia
E11	32	F	DEU	Europe	M. Sc.	5y	Academia

4 Designing Consent Mechanisms for Spontaneous Interactions

We conducted semi-structured interviews and design activities with experts to validate the scenario taxonomy and develop consent mechanisms for spontaneous AR interaction scenarios **(RQ2)**. The full interview guideline is available in the supplementary material. We obtained ethics approval in compliance with local regulations.

4.1 Participants

We used snowball sampling to recruit participants, enabling us to reach a specialized group of experts in privacy and AR. To qualify, participants needed to meet two criteria: 1) self-identify as privacy experts, and 2) either hold or pursue a Ph.D. in a privacy-related field. Moreover, we invited prospective participants to complete an online survey to validate their expertise, see Appendix Section A.2.1. We asked participants to self-assess their experience in eleven areas on a 5-point agree-disagree scale, see Table 3.

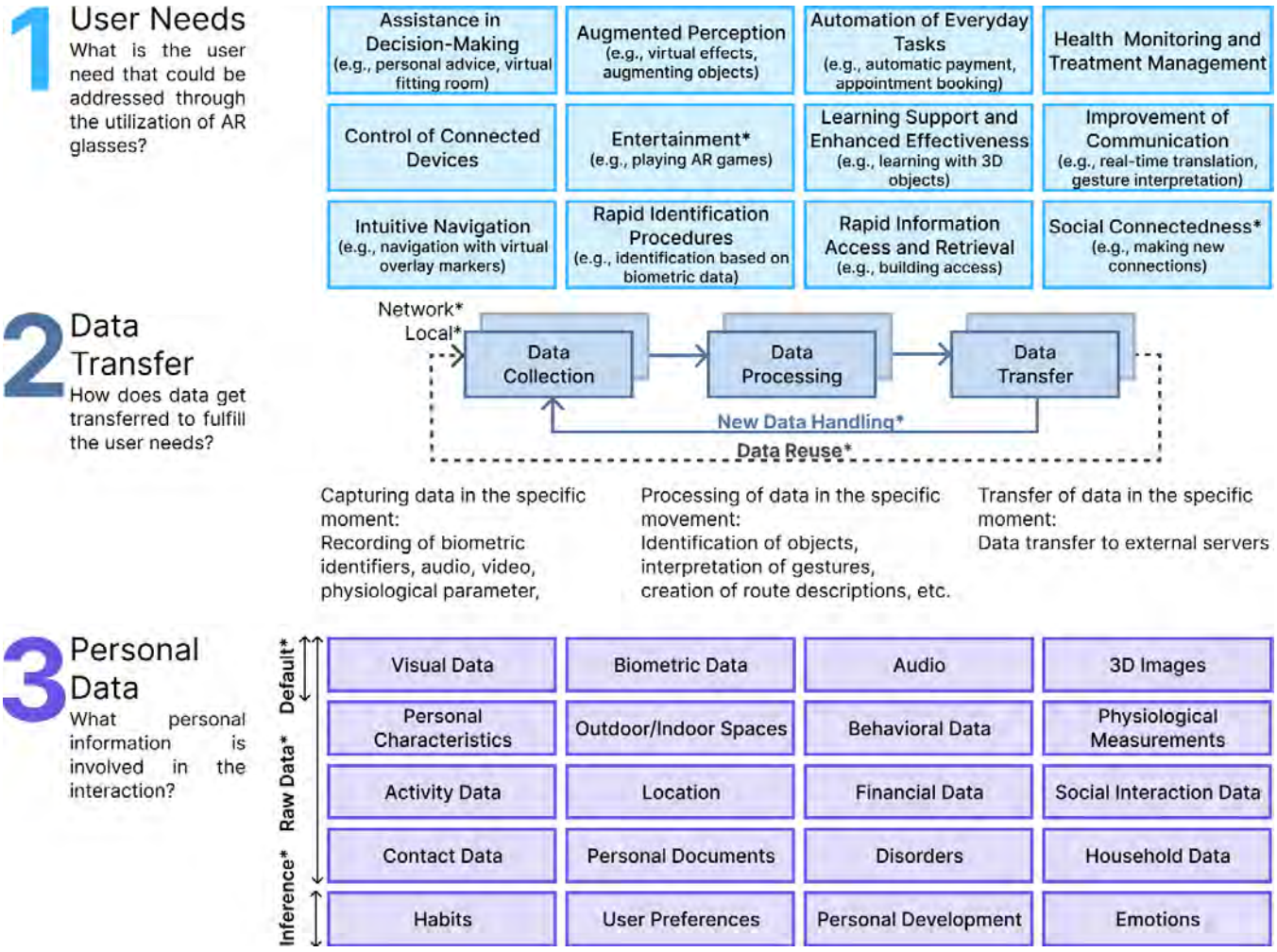

Figure 2: A scenario taxonomy for generating speculative privacy-sensitive AR interaction scenarios through the identified dimensions: *User Needs*, *Data Transfer*, and *Personal Data*. *User Needs* covers various AR applications such as decision-making or task automation. *Data Transfer* outlines stages of data flow, including data capture, processing, and transfer. *Personal Data* examines types of data involved, from default sensory data to inferred information. The elements marked with a * were adjusted in response to the expert interviews. We describe these adjustments in detail in Section 5.1.

We recruited eleven experts (see Table 2), comprising three women and eight men, aged 27 to 37 years ($M = 31$, $SD = 3.41$). Most experts ($N = 9$) were born in Europe, with one from Africa and one from Asia. Despite this diversity, the majority ($N = 9$) currently resided in Germany, while one lived in Canada and one in Switzerland. Ten experts worked in academia, and one worked in industry. Their experience in privacy-related roles ranged from one to eight years ($M = 3.7$, $SD = 2$).

4.2 Interview Protocol

Before the interview, we emailed our participants an informed consent form and a link to a demographic questionnaire. We conducted the interviews in person or via Zoom and structured the interview into two blocks, with the second block containing sketching tasks. When remote, we asked participants to show their sketches to the camera and send us a photo of the sketch after the interview.

In the first part, we aimed at discussing and validating the scenario taxonomy. For that, we familiarized our experts with the vision of everyday integrated AR glasses (i.e., a future where users accomplish their daily tasks and goals with the help of AR). Since we focus on the device user, we instructed the experts to disregard the bystander perspective. Furthermore, as the core of this study was spontaneous interactions, we thoroughly introduced them as events with a single purpose that, once executed, provide immediate contextual feedback to users. We also gave a concrete example of a shopping experience in a clothing store, where AR technology helps navigate customers around and displays interactive 3D visualizations, see Appendix Section A.3. We then explained the scenario taxonomy by linking all elements of the shopping example to the

Table 3: Experts' self-assessed expertise and practical experience rated on a 5-point scale for the following statement: "I am an expert in [research domain]." We asked about the following research domains: *Human-Computer Interaction (HCI)*, *Privacy (P)*, *Security Engineering (SE)*, *Interaction Design (ID)*, *Augmented Reality (AR)* and *Smart Home Technologies (SHT)*. We also assessed their professional experience in privacy-enhancing technologies *(EQ1)*, secure system architectures *(EQ2)*, augmented reality development *(EQ3)*, UI/UX design *(EQ4)*, and smart home technologies *(EQ5)*; see Appendix Section A.2.1 for the full questions.

EID	HCI	P	SE	ID	AR	SHT	EQ1	EQ2	EQ3	EQ4	EQ5
E1	■■■■■	■■■■□	■■■□□	■■■■□	■■□□□	■■□□□	■■■■■	■■□□□	■□□□□	■■■■□	■■□□□
E2	■■■■■	■■■■■	■■□□□	■■■■■	■■■■□	■■■■■	■■■■■	■■□□□	■■■□□	■■■■■	■■■■■
E3	■■■■■	■■■■□	■■■□□	■■■■□	■■■□□	■■□□□	■■■■■	■□□□□	■■□□□	■■■■■	■□□□□
E4	■■■■□	■■■□□	■■■■□	■■■■□	■■■■□	■■■□□	■■■□□	■■■□□	■■■■■	■■■■□	■■■□□
E5	■■■■□	■■■■■	■■■■□	■■■■□	■■■■□	■■□□□	■■■■□	■■■■□	■■■■■	■■■■□	■■□□□
E6	■■■■□	■■■■□	■■■■■	■■■■■	■■■■■	■■■■□	■■■□□	■■■□□	■■■■■	■■■■□	■■■■□
E7	■■■□□	■■■■■	■■■□□	■■□□□	■■■□□	■■■□□	■■■□□	■■□□□	■■□□□	■■□□□	■■□□□
E8	■■■■■	■■■■□	■■■□□	■■■■□	■■■■■	■■■■□	■■■□□	■■□□□	■■■■■	■■■■□	■■■□□
E9	■■■■■	■■■■□	■■■■□	■■■□□	■■□□□	■■□□□	■■■■□	■■■□□	■■□□□	■■■□□	■■□□□
E10	■■■■□	■■■□□	■■□□□	■■■■□	■■■□□	■■□□□	■■■□□	■■■□□	■■■■■	■■■■□	■■□□□
E11	■■■■□	■■■■■	■■■□□	■■■■□	■■□□□	■■■■□	■■■■■	■■■□□	■□□□□	■■■■□	■■■■□

elements of the taxonomy. We then asked the experts for feedback and potentially missing elements. Finally, we asked the experts to use the scenario taxonomy to create two interaction scenarios they considered particularly interesting and privacy-relevant. While they brainstormed their scenarios, we asked them to think aloud [47]. Finally, we asked the experts for each scenario to which extent, on a scale from 1 to 7, they agreed with the following statement: *"I think this scenario is very privacy concerning."*

In the second part, we asked the experts to sketch concrete consent mechanisms for the two scenarios they had developed during the first part of the interview. Before, we again highlighted the specific characteristics of spontaneous interactions, such as high daily repeatability and brief execution periods. As a concrete example, we declared privacy policies as inadequate consent mechanisms: from the user's perspective, engaging with long and complicated language proves inappropriate for providing short-term permission. With these specifications, we aimed to establish a general foundation and mutual reference point. We asked our participants to think aloud while sketching. Once they were finished, we asked for in-depth explanations of their designed mechanisms. We focused on what and how much information these mechanisms provide to users, when device owners receive privacy information, and how they can control their privacy decisions. We then asked the experts to reassess their previous privacy sensitivity scores for the scenarios, imagining that their privacy mechanism was in use. Finally, we asked them to share their thoughts on how suitable consent mechanisms might influence AR technology's general user experience and acceptance and for additional feedback or comments before we ended the interview. The interview lasted approximately one hour, and we compensated the experts with €12 per hour.

4.3 Data Analysis

We recorded 10.98 hours of audio data ($M = 59.9$ *min*, $SD = 5.1$), used Whisper for transcription, and Thematic Analysis [4] with Atlas.ti (v. 24.1.1) for analyzing the data. Two researchers independently open-coded two interviews, then met to resolve ambiguities and create a joint codebook. One researcher coded the remaining interviews, and a third researcher later joined to form code groups and overarching themes. All three researchers iteratively refined themes by comparing coded sections. We provide the codebook as supplementary material. All three researchers also systematically analyzed the experts' sketches by coding and categorizing elements within the sketches, identifying recurring patterns related to privacy consent mechanisms, and cross-referencing these with the experts' comments to understand their design choices.

5 Expert Interviews: Results

We identified five themes. *Reflections on the Scenario Taxonomy* captures the experts' feedback on the taxonomy, which we used to refine it. *Design Continuum of Consent Mechanisms* outlines the experts' proposed mechanisms for enabling privacy-preserving spontaneous interactions in AR environments. *Design Aspects* discusses practical considerations for implementing these mechanisms, while *Practicality Evaluation of Consent Mechanisms* summarizes participants' discussions on the feasibility and situational conditions for using the individual mechanisms. Finally, *Interplay between Privacy and User Experience* explores the conflict between privacy, user comfort, and control.

5.1 Reflections on the Scenario Taxonomy

All experts successfully created interaction scenarios using our taxonomy. They generally considered the taxonomy comprehensive and suitable for brainstorming and outlining interaction scenarios (E1, E2, E6, E8). However, the scenario creation process also uncovered missing components and opportunities for improvements. We marked all modifications and additions with an * in Figure 2. In the following, we detail these adjustments.

User Needs. E3 and E11 drafted use cases for entertainment purposes where users played AR games. As a fitting category was missing from the taxonomy, we added "Entertainment" as an additional user need. Further, E11 discussed situations where AR helps *"creating connections with other people, getting to know other people."* As a result, we added the new category "Social Connectedness." All other experts created scenarios that fit one of the user needs.

Data Transfer. E10 and E11 appreciated the separation of data transfer into a three-stage process. E11 stated that this would support developers in considering the extent to which privacy decisions influence functionalities: *"This [...] makes you stop and think about what different interactions you really have in which data is collected, [which helps you] identify, what happens if people, for example, restrict some kind of specific data."* Yet, E4 and E10 suggested visualizing the background processes regarding data processing and transfer by distinguishing between data usage on the devices and other connected appliances or systems via network communication. E4 illustrated it with an example of a shopping scenario: *"[W]hen the user enters the store[,] [...] it automatically loads his profile with the items that he bought the last time to give him suggestions [...]. This is happening via the internet, right? There's also another [data transfer] happening with a server."* Accordingly, we visualized data transfer in our design space at the network and local levels. As our experts also discussed scenarios where the system saved prior data input and applied it, for instance, for recommendations, we now differ between the handling of new data and data reuse. New data handling refers to direct data collection during an interaction, whereas data reuse refers to the reuse of data gathered in previous interaction scenarios.

Personal Data. E5 classified audio, video, biometric data, and 3D images as default required for AR's optimal functioning. E10 discussed introducing a differentiation between data directly collected and information inferred based on behaviors or multiple data sources, as E10 explained: *"the financial data is actual raw data [...]. But habits, you need to infer your habits."* As a result, we introduced a three-level classification as *Default*, *Raw Data*, and *Inferred Data*.

5.2 Design Continuum of Consent Mechanisms

Based on an in-depth analysis of the experts' designs, we divided the consent mechanisms into three categories: (1) **explicit**, (2) **semi-implicit**, and (3) **implicit**, see Figure 3. We adopted Corbett et al.'s [9] classification into implicit and explicit mechanisms and, thus, organized the mechanisms on a spectrum from explicit to implicit consent, reflecting various degrees of user effort and transferable consent. Generally, the user effort gradually decreases from left to right while the feasibility of transferable consent increases. This reflects a transition from active user involvement to a system-driven mechanism that automatically learns the user's privacy preferences and makes decisions on their behalf.

The experts outlined universal requirements that effective strategies should fulfill. As spontaneous interactions are characterized by multiple repetitions a day, they should not annoy the users. This could, for example, be achieved by implementing longer-lasting consent. Yet, whenever longer-lasting consent is given, there must be options to withdraw permissions easily (E3, E8). Several experts considered the non-intrusive design of the mechanisms challenging (E1, E3, E5, E7 - E11). E4 and E10 stressed the difficulty of explaining complex technical processes in simple terms, while *"not losing [the] information [...] needed for people to understand what's going on."* Information must be concise, as people's field of view is limited (E10). Overall, consent mechanisms should be *non-intrusive*, *easy to use*, and include *rapid access, execution, and modification*, *long-term consent for similar use cases*, and *compact and lightweight information provision*.

5.2.1 Explicit Consent Mechanisms. Experts proposed mechanisms that allow users to process a privacy notice directly. These mechanisms request the user's informed consent or refusal before using any data, leading to a high demand for user attention. The experts most often suggested mechanisms that used *gesture* (E1, E4, E7, E9, E10) and *voice* controls (E1, E2, E4, E6, E8, E10). Examples of gestures included nodding to agree with a data request (E1) or gestures that activate or deactivate sensor functions, such as simulating a camera trigger to control the video sensors (E4). Moreover, E10 suggested using gaze patterns, i.e., a sequence of eye movements to opt in or out: *"I first [l]ook here and then here as my consent pattern."* With *interaction-based* control, participants referred to using real-world objects to signal a privacy decision (E7, E9), such as rotating a product in a store to simultaneously provide consent: *"They could say, okay, turn left, I want to have more information [...] I give consent so that they can process my data."* Explicit consent mechanisms require direct user involvement, leading to increased cognitive load. Hence, we position explicit strategies on the left side of the continuum, with high user effort and low transferable consent, see Figure 3.

5.2.2 Semi-Implicit Consent Mechanisms. Semi-implicit consent mechanisms allow some automation, but users are kept in control, see Figure 3. For instance, E3 designed a *tangible mechanism* in the form of a privacy belt, see Figure 1a. The belt has several knobs that represent different types of personal data or data transfer stages. Users express their privacy preferences by turning these knobs. E3 imagined the interaction to become more seamless over time: *"In the beginning, they have to read the labels, but at some point, they know it by muscle memory."* E5 and E11 introduced physical sliders on the side of the AR glasses, where users can switch between different privacy data usage levels, and E6 and E11 suggested physical buttons to turn data recordings on or off, see Figure 1b. Here, experts suggested either binary on-and-off or granular multi-level switches (similar to the belt). As an even more granular option, E3 and E5 illustrated fine-grained control suitable for privacy belt and slider control, where the extent of the knob's rotation regulates the extent of data collection: *"So you can see, for example, that I'm roughly six foot tall, but you don't get that I'm exactly 183.2 cm"* (E3). Experts also suggested *virtual menus* that summarize all collected data or ongoing data usages in the user's field of view and offer immediate modification options (E3, E5, E9, E10). E5 discussed organizing these menus by filtering by location, specific scenarios, or sensitivity of a situation or context. E1 and E2 advocated for preset configurations, such as disabling all data collection and network connection at once or having buttons to activate, deactivate, pause, or delete data. To make it easier to use these menus, experts also suggested *companion devices* with conventional screens (E1, E3), see Figure 1c. Moreover, experts suggested *visualizing active data usage within sight*, for example, through icons (E1, E3, E6 - E8) or digital overlays on physical objects related to the used data, such as an overlay appearing directly on a sensitive document being viewed (E9), see Figure 1d. In summary, semi-implicit mechanisms require the user to define preferences at the beginning of the interaction. Unlike explicit mechanisms,

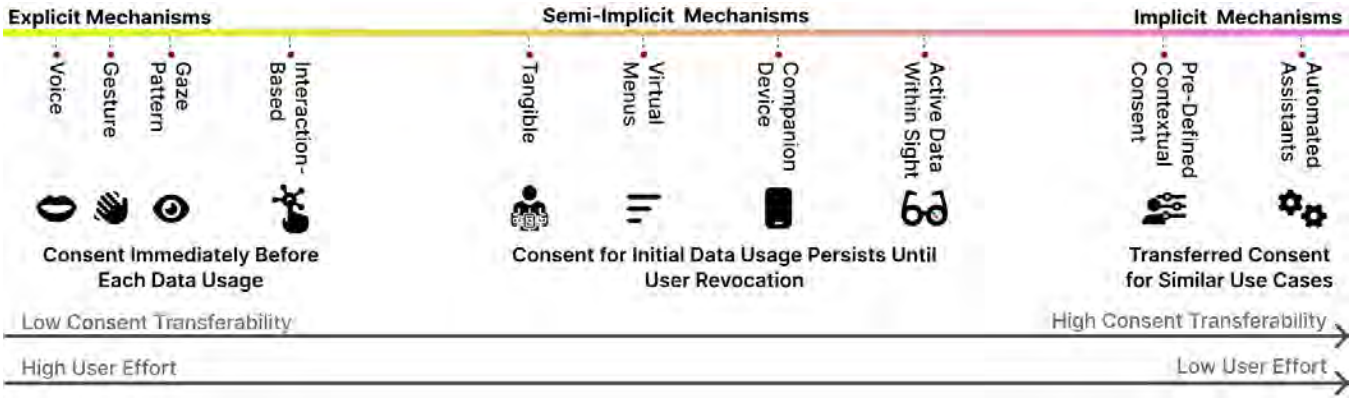

Figure 3: "Design Continuum" for privacy-preserving spontaneous interactions in AR: Allocation of explicit, semi-implicit and implicit mechanisms on a scale between explicit and implicit consent with the associated sub-mechanisms.

the permissions are transferable to use cases further until the user intervenes. Users would then evaluate permissions as soon as a contextual change is detected.

5.2.3 Implicit Consent Mechanisms. Most experts (E1 - E7, E9, E10, E11) discussed implicit, context-sensitive mechanisms, where the mechanism analyzes and compares the individual contexts of different interaction scenarios and automatically adapts settings based on user-defined privacy settings. Over time, the mechanisms learn the users' preferred decisions regarding their privacy and thus adjust settings autonomously without requiring user intervention.

Concretely, experts suggested *Contextual Consent based on (Pre-)Defined User Preferences* (E1, E2, E4, E5, E6, E7, E10) and *Automated Assistants* (E2, E9, E11). For example, E6 described a location-based mechanism with pre-defined privacy zones: *"Once you enter this area, the system presents you with a pop-up that allows you to decide what you want to share in terms of personal data."* Since privacy areas can overlap, E6 suggested defining general permissions for similar activities, such as restaurant visits. Yet, E10 emphasized that GPS information is not precise and suggested that camera-based scene understanding could improve accuracy. E5, E1, and E7 also suggested restricting authorizations based on activities, location, or sensitivity levels. Users could, for example, curate a profile for leisure and one for professional purposes (E5). E1 further suggested the implicit mechanisms could be simulated in VR to foster user acceptance. Users could experience scenarios in virtual environments and make privacy decisions according to their perception. As implicit mechanisms rely on preset privacy profiles or learned user behavior to adapt to similar contexts, they reduce user burden but require users to trust the system-driven settings. Consequently, we classified these mechanisms on the right side of the continuum with low user effort and high consent transferability; see Figure 3.

5.3 Design Aspects

Based on the discussions and expert sketches, we abstracted the following design aspects, shown in Figure 4: *Consent Triggers*, *Awareness Cues*, *Interaction Modalities*, *Visualizations*, and *Time Frames*.

5.3.1 Consent Trigger. For all mechanisms, except explicit ones, a trigger is required to start the consent process. Experts suggested using context changes as triggers (E2, E5 - E11), such as entering a new location (E5, E6, E8, E10), interacting with a sensitive document like a personal letter (E9), or the presence of a bystander (E10). They also proposed learning repetitive behaviors, such as consistently allowing the sharing of financial information and automatically applying consent to similar situations (E1, E2, E9, E11). Physiological cues, like a high heart rate indicating discomfort, could also trigger a consent interaction (E4, E7). Additionally, experts recommended scheduling periodic consent reviews to ensure learned behaviors still align with user expectations (E2, E7, E8, E11). Lastly, a trigger could occur when preferences clash with data practices, such as collecting data types exceeding users' comfort levels (E3, E5, E10).

5.3.2 Awareness Cue. Once a consent interaction is triggered, the system must attract the user's attention to get them to interact with the mechanism. For that, experts suggested visual augmentations, such as overlaying the whole environment or objects with a specific color or icons (E7, E9) or blinking lights at the periphery of the field of view (E1, E11). Other suggestions were to use haptic feedback, such as vibrations (E6, E9, E11), audio feedback, such as the glasses explaining what kinds of data get collected and processed (E9, E10), or simple pop-up notifications (E1, E2, E6, E10, E11).

5.3.3 Interaction Modalities. Users can interact with the consent mechanism in various ways. The experts frequently mentioned GUI interactions, such as dragging, scrolling, tapping, or toggling visual overlays, such as icons (E1 - E5, E7, E8), see Figure 5. Experts also suggested mid-air gestures, such as accessing privacy menus by performing pinch gestures (E4, E5) or other specialized gestures that users would otherwise not perform (E2, E4, E7, E9). Other suggestions were to have gaze-based interaction, where a menu item gets selected when the user looks at it for a longer time (E2, E5, E9), or physical interactions where the user interacts with buttons (E3, E4, E6, E11) or sliders (E5, E11). Finally, experts suggested voice interactions, such as specialized wake words (E2) or natural speech (E4, E5, E9).

Consent Trigger	Awareness Cue	Interaction Modalities	Visualizations	Time Frames
Context Change (e.g., entering new location)	Visual Augmentation (e.g., overlay physical environment)	GUI Interaction (e.g., dragging, scrolling, 3D object manipulation)	Active Data Usage (e.g., virtual LEDs, animated 3D bubbles)	Decision Timeout (e.g., 5 sec. to accept or deny data usage)
Physiological Abnormalities (e.g., high heart rate)	Haptic (e.g., vibrations)	Mid-Air Gestures (e.g., pinch gesture, thumbs up gesture)	Data Flow (e.g., data transfer)	Consent Validity (e.g., consent applies for 6 months)
Repetitive Behavior (e.g., user always declines financial data)	Audio	Gaze-Based Interaction (e.g., dwell time)	Consequences (e.g., icon per data type)	
Scheduled Consent Reviews (e.g., pop-up after x weeks)	Pop-Up Notifications	Physical Interaction (e.g., button, slider)		
User-Defined Preferences (e.g., exceeding comfort level)		Voice (e.g., wake words)		

Figure 4: The different design aspects of the experts' mechanisms for consent in AR environments.

5.3.4 Visualizations. Experts proposed various elements for visualization in consent mechanisms. Many emphasized active data visualizations, using virtual LEDs (E1, E4, E11) or dynamic icons and bubbles that light up, change color, or shift shape when data is in use (E1, E8, E11). Some described animated 3D bubbles that change speed and size to represent data activity (E3, E7, E8). Others focused on visualizing data flow, employing 3D models (E1) or overlays like bubbles and icons to show data transfers to external providers (E4, E7, E9). E6 stressed the need to illustrate the consequences of data sharing to improve understanding and awareness.

5.3.5 Time Frames. To minimize disruption from notifications when explicitly making decisions, for example, as they might block the users' field of view (E2), experts discussed implementing time limits in which users must grant their permission (E1, E2, E7, E8). As a result, the notifications would automatically disappear if users do not interact (E2), and an automated confirmation or rejection would occur (E1, E7). Another feature relates to validity periods for privacy decisions. When users define privacy preferences, they can define a time frame for which the decision should persist, such as the next 15 minutes or the whole month (E1 - E3, E6, E8).

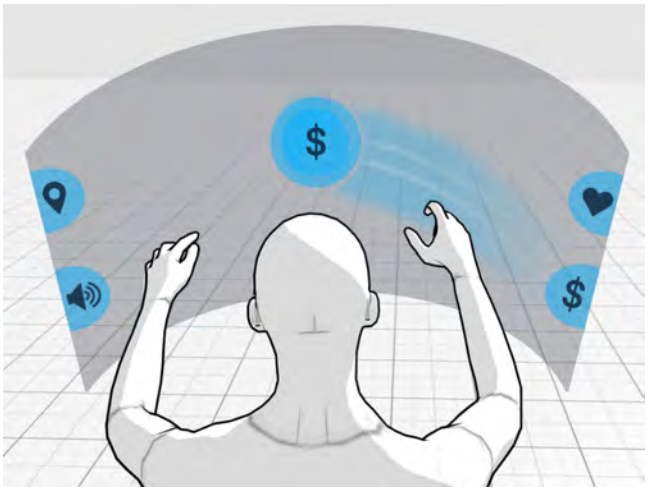

Figure 5: E3's envisioned interaction with icons to toggle consent per data type.

5.4 Practicality of Consent Mechanisms

The experts distinguished between dynamic and static contexts (E6, E10). Dynamic contexts describe scenarios involving multiple locations, such as biking (E10). Similarly, E6 addressed the difference between dynamic and static situations by extending the discussion on the frequency and sensitivity of data requests: *"I give access [to] my documents. Now, [...] one of my colleagues sends me a new confidential document. Does it mean now that the system still has access to my documents?"* E6 further discussed that the higher the sensitivity of personal data, the more likely they are to accept alerts and wish to customize their privacy setups actively. Moreover, experts differentiated between trusted and untrusted spaces (E3, E4). They argued that voice and gesture control are unsuitable for managing data in public (E1, E2, E4) as spoken privacy alteration could trigger uncertainty among bystanders about why a person wants to change their settings (E2), and performing gestures might be perceived as weird (E1, E3, E10). In contrast, the privacy belt can enable subtle control in all environments: *"If I know where those buttons are, changing my privacy settings or changing what I'm transferring is a very subtle movement"* (E3). Experts avoided using noticeable consent mechanisms in public settings but considered them acceptable in private spaces (E4). E3 further noted that the presence of unfamiliar people could turn trusted spaces into untrusted ones, prompting individuals to restrict their privacy settings further.

Based on these discussions, we extract the following contextual factors: The *frequency of location or scene modifications*, the *frequency of data requests*, the *sensitivity of the information*, and the *trust level of the environment*, influenced by public vs private spaces and the presence of other people. We synthesized these insights into a flowchart, see Figure 6.

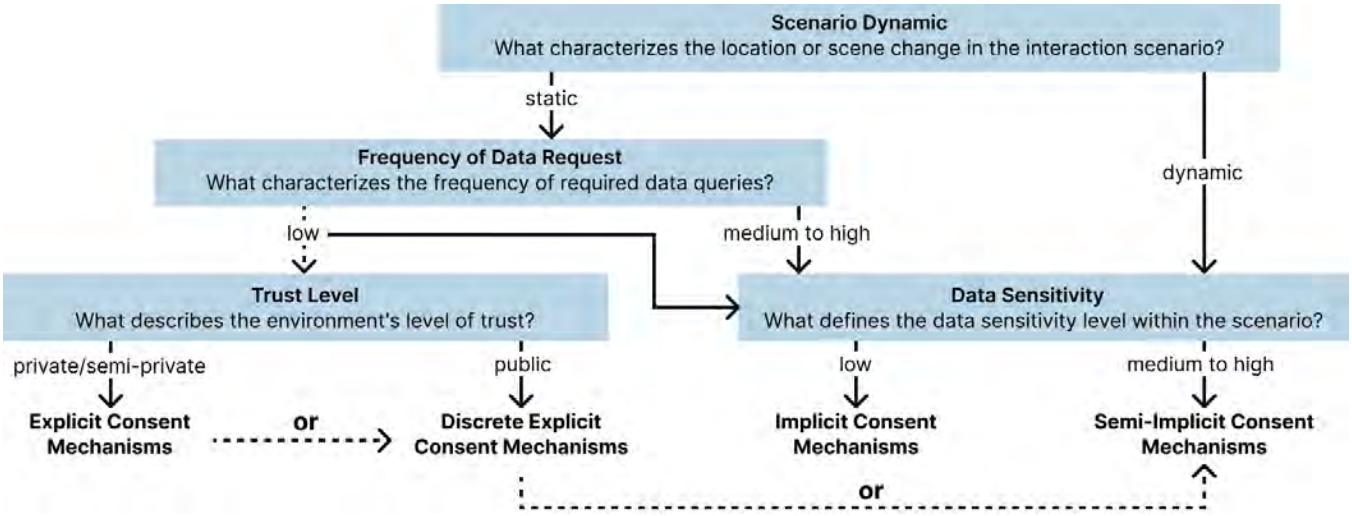

Figure 6: A flowchart to decide on suitable mechanisms. The dotted arrows indicate a choice between mechanisms.

5.5 Interplay Between Privacy and User Experience

Most people prefer dealing with privacy settings in the background to avoid interfering with their primary tasks (E4, E8, E10). Furthermore, privacy concerns fade into the background whenever users benefit from using technology to fulfill their needs (E9, E10). Accordingly, consent mechanisms should maintain the user's focus on task execution. When comparing AR consent strategies with previous technologies, the experts discussed that smartphone applications primarily ask users to approve sensor capabilities and data collection once during installation (E4 - E6, E9, E10), which conflicts with the need to manage privacy settings in a real-time, context-sensitive manner. Hence, one-time consent without further active involvement is insufficient to guarantee privacy. Consequently, the experts discussed the trade-off between comfort and user involvement and between automation and user control. Further, E1 and E11 associated automated decision-making with restricting users' autonomy (E11): *"[L]ess decision means less privacy because users are less aware of [the privacy choice]"* (E1). A high automation level requires more data collection, highlighting the dark side of advanced privacy technologies (E1, E11). Nonetheless, E3 and E11 considered adaptive systems combined with awareness triggers as a good middle ground. Here, awareness triggers allow manual intervention, which maintains the user's decision-making autonomy.

Based on these insights, we developed a privacy trade-off panel for consent mechanisms as shown in Figure 7. The x-axis represents the progression from active user consent to automatic system consent, while the y-axis reflects users' sense of control, ranging from low to high. We plotted each consent mechanism along these axes to illustrate its trade-off between user control and convenience. Explicit consent mechanisms, represented by the diamond in the upper left, allow users to make intentional decisions for each data request, providing high control but requiring high effort. Semi-implicit consent mechanisms, represented by the triangle in the upper middle, offer users flexibility to transfer consent to similar scenarios, with the option for user-initiated interventions at any time. This positions them between active and automated decisions, maintaining a high level of control with moderate effort. For implicit mechanisms, we distinguished between two strategies based on expert input. The green square represents implicit user predefined mechanisms, where users set preferences initially, and the system then applies these to relevant contexts. While this approach offers medium control due to the system's automatic application of user-defined settings, it requires less frequent user intervention than explicit mechanisms. Finally, automated implicit mechanisms, represented by the blue circle in the lower right, learn from user behavior over time. As the system autonomously makes privacy decisions, users must trust it to interpret their privacy preferences accurately, resulting in low user control but high convenience. The dotted lines in the figure further illustrate the trade-off: general user effort decreases as control shifts from active consent to automated consent, while user comfort generally increases with automation. This panel, therefore, visualizes the balance each mechanism strikes between user involvement, control, and convenience.

6 Discussion

In the following, we discuss our findings and explain how our six conceptual tools, i.e., the scenario taxonomy (Figure 2), design continuum (Figure 3), design aspects (Figure 4), flowchart (Figure 6), privacy trade-off panel (Figure 7), and prediction chart (Figure 8), can be combined to form a framework for designing effective consent mechanisms for spontaneous AR interactions.

6.1 The Right Consent Mechanisms Depend on the Context

The experts identified scenario dynamics, frequency of data requests, data sensitivity, and trust level (see Figure 6) as contextual factors influencing the appropriateness of consent mechanisms. This strongly resonates with Nissenbaum's theory of contextual

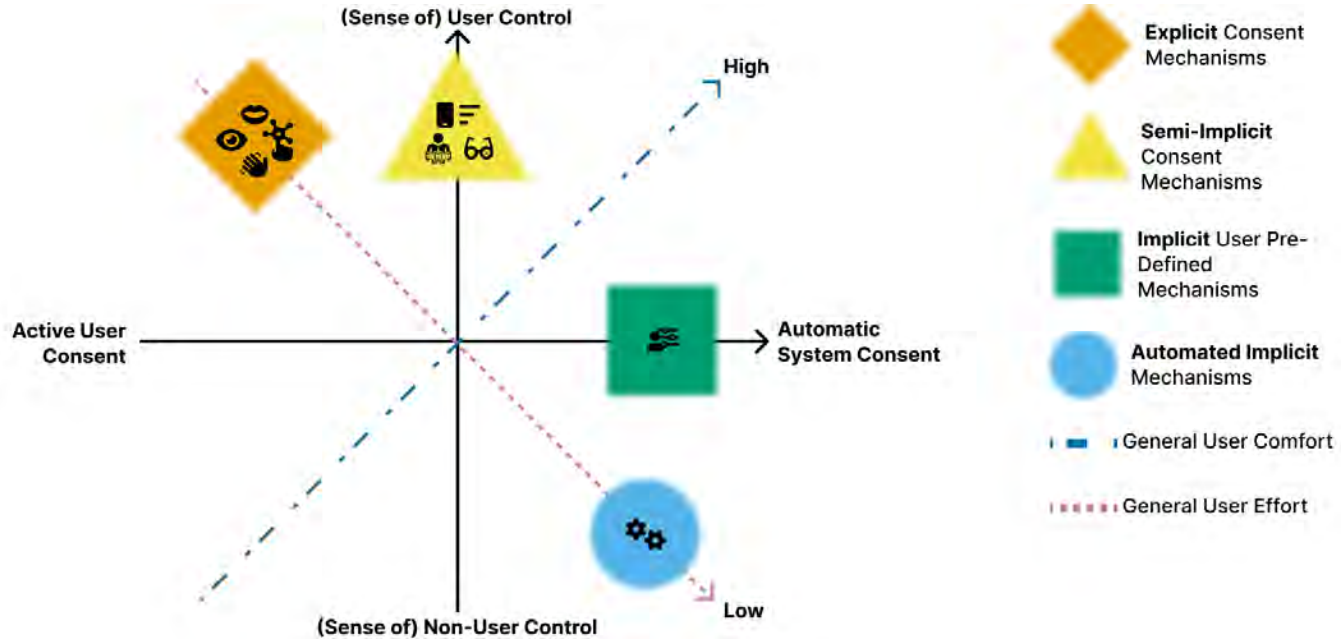

Figure 7: Privacy trade-off panel for consent mechanisms in AR. The x-axis shows the progression from active user consent to automatic system consent, while the y-axis indicates the users' sense of control from low to high. Explicit consent mechanisms (diamond) provide high control but require high user effort. Semi-implicit mechanisms (triangle) allow flexible user interventions with moderate effort. Implicit user pre-defined mechanisms (square) offer medium control after initial setup. Automated implicit mechanisms (circle) provide low control but high convenience. The dotted lines represent the trade-off between user comfort (increasing with automation) and user effort (decreasing with automation).

integrity [33–35], which indicates that privacy gets violated when data practices do not align with the norms of a situation.

The experts differentiated between static and dynamic scenarios and suggested that explicit mechanisms might be suitable in static scenarios, where activities and locations remain constant, which leads to fewer privacy notifications. However, even in static contexts, transferable consent mechanisms might be better suited whenever frequent data requests become necessary, such as in an office environment where trusted company data is shared continuously (E6). In dynamic scenarios, where locations and activities change frequently, transferable consent mechanisms are particularly effective at reducing repetitive privacy requests and mitigating the risk of information overload. Such scenarios can overwhelm users [28]. Data sensitivity is another important factor: for sensitive data, semi-implicit mechanisms provide users with control to review and modify settings, while implicit mechanisms are suitable for data users consider less sensitive, offering convenience with minimal risk when user preferences are occasionally misaligned. Trust level also plays a critical role. In private or semi-private environments, explicit consent mechanisms are appropriate. In public environments, however, discrete explicit or semi-implicit mechanisms are preferred to avoid social discomfort or security risks, such as being observed while adjusting privacy settings [25].

Overall, experts preferred semi-implicit and implicit mechanisms, as they balance user comfort and efficiency. Explicit mechanisms, while less favored, remain viable alternatives depending on the spatial, social, and contextual conditions.

6.2 Consent Mechanisms Influence Users' Perceived Control

Based on the experts' discussions around user control and the advantages and disadvantages of different approaches, as well as our own analysis and insights from related work, we developed a prediction chart that models users' perception of consent mechanisms over time (see Figure 8). The chart visualizes how mechanisms balance active user decisions and automated system decisions, affecting perceived control. The x-axis represents the spectrum from user-controlled to system-controlled decisions, while the y-axis shows the degree of perceived control, ranging from low (bottom) to high (top). Solid lines depict how users' perceived control evolves over time for each mechanism, with squares indicating specific moments when contextual changes or triggers may affect this perception.

Explicit consent mechanisms require user permission before a system uses data. Since explicit consent is granted at a specific moment and remains static, it has no dynamic progression over time and is not depicted in the chart.

In the case of *semi-implicit consent mechanisms* (yellow), the user makes their initial privacy decisions, which remain valid until they revoke or change them. However, users can revise these decisions if they notice a privacy-relevant context change while using the device. This approach allows semi-implicit mechanisms to actively

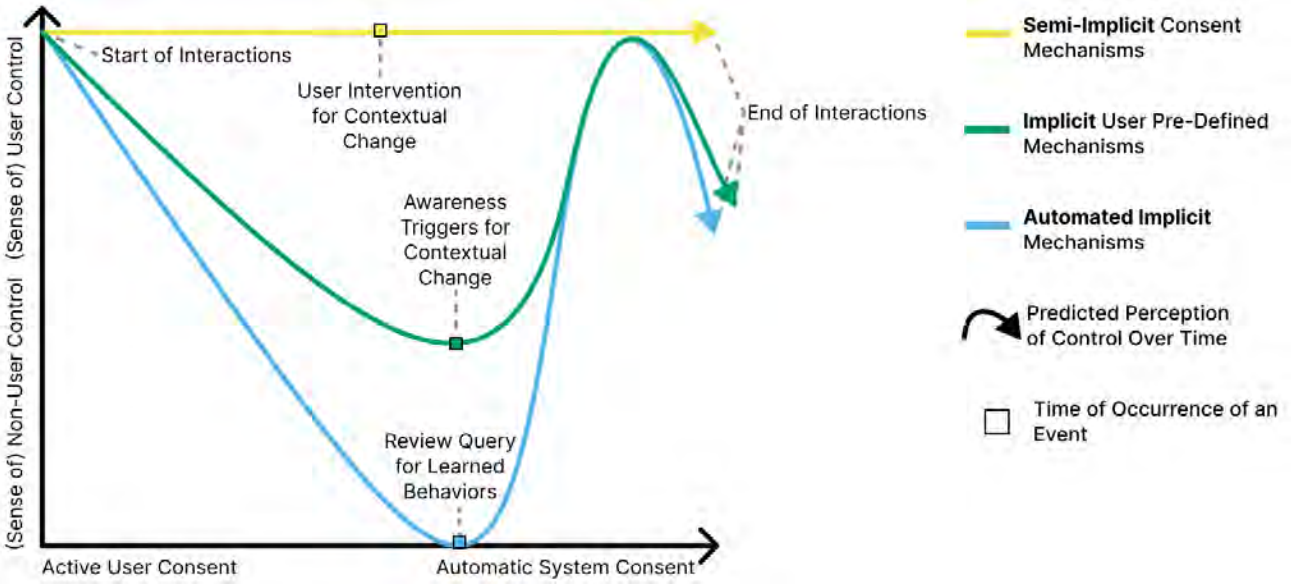

Figure 8: The prediction chart predicts the perception of user control over time across three consent mechanisms: Semi-Implicit, Implicit User Pre-Defined, and Automated Implicit. The x-axis represents the transition from Active User Consent to Automatic System Consent, while the y-axis shows the range from user to non-user control. The arrows represent the time from the start of the interaction to the end. Key events that influence control dynamics are marked with squares.

support the user by enabling manual intervention at any time. As a result, we predicted a consistently high level of perceived control over time, reflecting a strong sense of user control balanced between active and automated consent.

For *implicit user pre-defined mechanisms* (green), the system automatically makes privacy decisions when it detects a privacy-relevant context change. Implicit user pre-defined mechanisms require users to specify their choices beforehand. The system then applies these preferences automatically to similar use cases, meaning users rely on the system to interpret situations accurately based on their preferences. However, users can verify and override system-driven decisions through awareness triggers. When a trigger activates, control temporarily returns to the user, allowing them to adjust the system's decision. As a result, we predict that the user's sense of control increases at the point of trigger activation.

Automated implicit mechanisms (blue) learn from users' situational behavior, allowing the system to determine future privacy practices autonomously. This requires users to trust that the system will accurately interpret their behavior and make appropriate decisions. Research by Colnago et al. [6] found that users often associate automated decisions with a loss of control, while Stöver et al. [51] showed discomfort with computer-guided learning, as past behavior may not reflect current needs. Consequently, we predict a decline in users' sense of control over time. To address this, experts suggested periodic reviews, allowing users to verify and adjust the system's decisions. These reviews temporarily boost perceived control, which then declines again as the system resumes autonomous decision-making until the next trigger.

In summary, mechanisms that reduce user effort through automation increase comfort but may limit the sense of autonomy [6]. Our prediction chart underscores the importance of control and transparency in implicit mechanisms. Users need to understand system decisions and retain the ability to adjust them when necessary. Active participation, such as frequent privacy queries or confirmation requests that are thoughtfully designed to balance user engagement and automation can enhance acceptance without causing annoyance. Transparent summaries via menus or dashboards could further support user understanding and trust [51].

6.3 A Conceptual Framework: Combining the Six Tools

Our six tools, i.e., the scenario taxonomy (Figure 2), design continuum (Figure 3), design aspects (Figure 4), flowchart (Figure 6), privacy trade-off panel (Figure 7), and prediction chart (Figure 8), form a cohesive framework for designing effective consent mechanisms for spontaneous AR interactions.

Schaub et al. [46] developed a design space for effective privacy notices, focusing on the dimensions of timing, channel, modality, and control. Our framework builds on and extends this space by applying these dimensions to spontaneous AR interactions. The flowchart (Figure 6) addresses both timing and channel dimensions. For timing, it links scenario dynamics and data request frequency to appropriate consent mechanisms, recommending explicit mechanisms for "at setup" notices in static scenarios and semi-implicit or implicit mechanisms for "just-in-time" or "context-dependent" notices in dynamic contexts. For channel, it provides contextual recommendations, such as using discrete explicit or semi-implicit mechanisms to minimize discomfort in public settings, while relying on explicit mechanisms to enhance transparency in private contexts. While Schaub et al. [46] emphasizes modalities such as

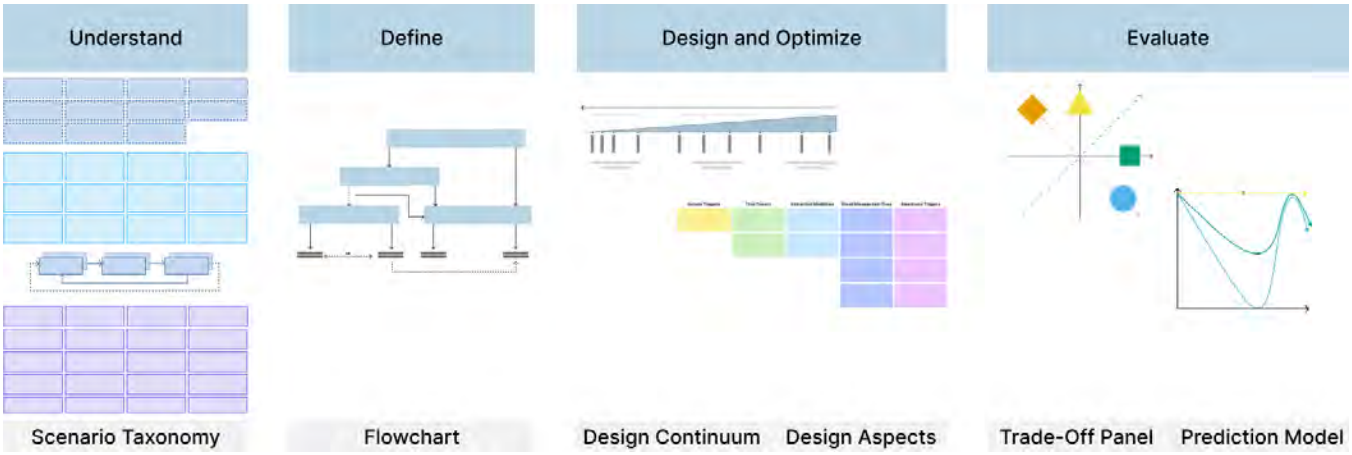

Figure 9: Our conceptual framework shows how our six tools fit into the four phases of the UCD.

visual, auditory, or haptic, our design aspects (Figure 4) and trade-off panel (Figure 7) enables designers to refine and evaluate these choices in terms of user effort and perceived control, providing practical tools for selecting the most appropriate modality for AR interactions. Additionally, we expand on Schaub et al. [46] control types by demonstrating how explicit, semi-implicit, and implicit consent mechanisms influence user comfort and decision-making.

We now outline how our tools form a comprehensive framework by linking each to a phase of the user-centered design (UCD) process [1], see Figure 9. The scenario taxonomy (Figure 2) fosters understanding of privacy-relevant spontaneous interactions in AR that require effective consent mechanisms. After generating the interaction scene, our flowchart (Figure 6) helps specify contextual requirements to select appropriate consent mechanisms. In most cases, semi-implicit and implicit mechanisms are the optimal choice due to their ability to transfer consent to similar use cases. Thus, they reduce the risk of information and cognitive overload. However, we anticipate explicit mechanisms with higher user involvement as an alternative solution whenever the situations are static and do not involve too many privacy decisions. Next, the design continuum (Figure 3) helps select concrete mechanisms across the spectrum from explicit to implicit, and using the design aspects (Figure 4), the mechanisms can be enhanced and optimized. Finally, the trade-off panel (see Figure 7) evaluates and compares mechanisms according to their impact on the user experience by evaluating the required user involvement and the resulting control. As an expansion, the prediction chart (Figure 8) demonstrates the expected change in the user's sense of control when applying a particular consent mechanism. Yet, this process is not linear. We rather expect multiple revisions and iterations. Future implementation and user tests in natural environments will allow obtaining feedback from users and observing how they interact with the mechanisms. These insights can then validate or reject our assumptions and introduce necessary refinements to our framework.

6.4 Multi-level Cooperation of Legal Institutions, NGOs, and Companies for Effective Data Protection

As AR glasses become everyday companions, robust legal frameworks are crucial for privacy protection. We propose redesigning user-oriented measures for consent, transparency, and data control as a starting point for research. However, data protection requires more than consent mechanisms or privacy-by-design solutions. Coordinated efforts by legal institutions, NGOs, and companies are essential. In 2022, the European Commission acknowledged that current rights fail to address digital society's needs, calling for shared responsibility among stakeholders [7]. Similarly, Jerome and Greenberg [23] urged companies to implement clear data policies and user-friendly privacy settings. These initiatives underscore the importance of standardized protections and reinforce our focus on AR-specific consent mechanisms. A recurring challenge [50] is: Are privacy mechanisms in AR realistic or utopian? Companies may resist privacy features that limit data access, prioritizing privacy-by-policy over privacy-by-design to enable continued data collection [50]. Invasive AR products could soon push privacy limits. Thus, aligned with the EU declaration [7], stricter regulations should be imposed to encourage companies to adopt user-centric privacy protections. Legal frameworks, such as the General Data Protection Regulation (GDPR) [13], must adapt to immersive technologies, balancing functionality with user privacy. Nissenbaum [33–35] emphasizes that effective data management requires collaboration among all stakeholders. Yet, in a future where people are constantly monitored and data is continuously generated, can individuals retain control over their data? Moreover, AR impacts bystanders, further complicating privacy concerns. These challenges call for user-centric data protection regulations that foster user-centered technology development through research that works for and with users [42].

6.5 Limitations and Future Work

We recruited laypersons for our focus groups as the exploratory nature of our research questions called for a method that generated

speculative ideas and fostered exchanging opinions [4, 53]. While the small group size limits generalizability, we included participants with diverse AR experiences to represent the target audience broadly. Yet, future studies should also involve experts to provide new perspectives and uncover overlooked dimensions.

We provided focus group participants with an example interaction scenario to familiarize them with the research topic. Despite efforts to present the material vaguely and without bias, some anchor effects were unavoidable, where people rely on previously provided information as a reference point when making decisions [14]. For instance, virtual navigation appeared in every description, reflecting elements of the example scenario. Additionally, speculative design methods risk eliciting responses and behaviors that may not align with participants' actual behavior [27].

Overall, we hope to have generated a comprehensive design space for privacy-sensitive AR interaction scenarios. However, we acknowledge that not all possible scenarios may be captured. We view the taxonomy as a starting point for further exploration and refinement. For instance, adding a dimension to describe the user's immediate environment could enhance its scope. Experts noted that the privacy sensitivity of AR interactions is influenced by factors such as the user's location or the presence of others. While these aspects were analyzed in our flowchart, incorporating them into the taxonomy could be valuable for future work.

We used snowball sampling to recruit the experts for the interviews. While this allowed us to access a specialized group of experts, it also introduced the potential for selection bias, as participants were initially recruited through personal networks, which may have affected sample diversity and generalizability of the findings.

The consent mechanisms proposed by the experts were partially shaped by the capabilities of current technology and existing privacy regulations. However, advancements in AR technology and the evolution of data protection laws will likely reshape how users manage privacy and use AR glasses. Notably, AI advancements could significantly expand AR application scenarios, introducing new interactions and privacy challenges. Future research on consent mechanisms for spontaneous AR interactions may uncover innovative solutions. We, therefore, recommend revisiting this study in a few years with a focus on technological progress.

We used Likert items to assess the experts' expertise, experience, and privacy concerns regarding their envisioned interaction scenarios. To mitigate the tendency toward agreement bias, we included a neutral option to encourage more deliberate responses [11]. However, despite these precautions, we acknowledge that some responses may still reflect a degree of agreement bias.

Finally, extending the focus from primary device users to bystanders introduces new research questions: How can both device users and bystanders manage privacy and protect their information? How can bystanders express their privacy preferences during spontaneous interactions? We recommend exploring future AR interaction scenarios involving both groups, with an emphasis on effective permission strategies. Developing consent mechanisms that safeguard the privacy of all parties could improve the social acceptance of AR technologies and foster new social norms.

7 Conclusion

Based on the focus groups and expert interviews, we created six conceptual tools: (1) a scenario taxonomy that enables the generation of privacy-relevant spontaneous AR interaction scenarios; (2) a flowchart that evaluates situational characteristics of scenarios to identify appropriate consent strategies; (3) a design continuum to decide on a concrete mechanism; 4) the design aspects to optimize the mechanisms by strengthening user control; (5) a privacy trade-off panel to evaluate the effectiveness of the mechanisms, i.e., their impact on user effort, control, and comfort in particular use cases; and, finally, (6) the prediction chart which hypothesizes how users perception of the mechanisms evolves regarding their decision-making autonomy and sense of control. Together, the tools form a conceptual framework that supports developers and designers in creating effective consent mechanisms for spontaneous AR interaction scenarios.

8 Open Science

We provide all focus group and interview material in the supplementary material and on the Open Science Framework: https://osf.io/ukxw7/

References

[1] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. 2004. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications* 37, 4 (2004), 445–456.

[2] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 89 (sep 2018), 27 pages. doi:10.1145/3264899

[3] Marica Bertarini. 2014. *Smart glasses: Interaction, privacy and social implications.* Student Report. ETH Zurich, Department of Computer Science, Zurich, Switzerland. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=35867081685ff40ea0b245d315b2d54e42235b69

[4] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI Research: Going Behind the Scenes.* Springer Cham, Cham, Switzerland. 51–60 pages. doi:10.2200/S00706ED1V01Y201602HCI034

[5] Ji Won Chung, Xiyu Jenny Fu, Zachary Deocadiz-Smith, Malte F Jung, and Jeff Huang. 2023. Negotiating Dyadic Interactions through the Lens of Augmented Reality Glasses. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 493–508. doi:10.1145/3563657.3595967

[6] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376389

[7] Europese Commissie. 2022. European Declaration on Digital Rights and Principles for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

[8] Crystal Connors, Sean P. Theonnes, and Shane Pase. 2013. Privacy and Security in an Augmented World. In *National Social Science Proceedings*, Vol. 53. National Security Space Association, San Francisco Summer Seminar, 15.

[9] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y. Charlie Hu, and Bo Ji. 2023. BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems. In *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services* (Helsinki, Finland) *(MobiSys '23)*. Association for Computing Machinery, New York, NY, USA, 370–382. doi:10.1145/3581791.3596830

[10] Matthew Corbett, Brendan David-John, Jiacheng Shang, Y. Charlie Hu, and Bo Ji. 2024. Securing Bystander Privacy in Mixed Reality While Protecting the User Experience. *IEEE Security & Privacy* 22, 1 (2024), 33–42. doi:10.1109/MSEC.2023.3331649

[11] James T Croasmun and Lee Ostrom. 2011. Using likert-type scales in the social sciences. *Journal of adult education* 40, 1 (2011), 19–22.

[12] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2377–2386. doi:10.1145/2556288.2557352

[13] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://data.europa.eu/eli/reg/2016/679/oj

[14] Adrian Furnham and Hua Chu Boo. 2011. A literature review of the anchoring effect. *The Journal of Socio-Economics* 40, 1 (2011), 35–42. doi:10.1016/j.socec.2010.10.008

[15] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative Privacy Concerns about AR Glasses Data Collection. *Proceedings on Privacy Enhancing Technologies* 2023, 4 (2023), 416–435. doi:10.56553/popets-2023-0117

[16] Mark A. Graber, Donna M. D'Alessandro, and Jill Johnson-West. 2002. Reading level of privacy policies on internet health web sites. *Journal of Family Practice* 51, 7 (2002), 642–642.

[17] Jason Hong. 2013. Considering privacy issues in the context of Google glass. *Commun. ACM* 56, 11 (nov 2013), 10–11. doi:10.1145/2524713.2524717

[18] Jinhan Hu, Andrei Iosifescu, and Robert LiKamWa. 2021. LensCap: split-process framework for fine-grained visual privacy control for augmented reality apps. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services* (Virtual Event, Wisconsin) *(MobiSys '21)*. Association for Computing Machinery, New York, NY, USA, 14–27. doi:10.1145/3458864.3467676

[19] Yuming Hu, Mingyu Zhu, Qiao Jin, Feng Qian, and Bin Li. 2023. MagicCloth: Protect User Privacy in AR Streaming. In *Proceedings of the 1st ACM Workshop on Mobile Immersive Computing, Networking, and Systems* (Madrid, Spain) *(ImmerCom '23)*. Association for Computing Machinery, New York, NY, USA, 222–228. doi:10.1145/3615452.3617936

[20] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. 2013. Enabling Fine-Grained Permissions for Augmented Reality Applications with Recognizers. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 415–430. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jana

[21] Suman Jana, Arvind Narayanan, and Vitaly Shmatikov. 2013. A Scanner Darkly: Protecting User Privacy from Perceptual Applications. In *2013 IEEE Symposium on Security and Privacy*. IEEE, New York, NY, USA, 349–363. doi:10.1109/SP.2013.31

[22] Jk Jensen, Jinhan Hu, Amir Rahmati, and Robert LiKamWa. 2019. Protecting Visual Information in Augmented Reality from Malicious Application Developers. In *The 5th ACM Workshop on Wearable Systems and Applications* (Seoul, Republic of Korea) *(WearSys '19)*. Association for Computing Machinery, New York, NY, USA, 23–28. doi:10.1145/3325424.3329659

[23] Joseph Jerome and Jeremy Greenberg. 2021. Augmented Reality+ Virtual Reality Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds. *Washington DC USA* (2021).

[24] Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie Kaufman. 2023. Erebus: Access Control for Augmented Reality Systems. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 929–946. https://www.usenix.org/conference/usenixsecurity23/presentation/kim-yoonsang

[25] Marion Koelle, Swamy Ananthanarayan, Simon Czupalla, Wilko Heuten, and Susanne Boll. 2018. Your smart glasses' camera bothers me! exploring opt-in and opt-out gestures for privacy mediation. In *Proceedings of the 10th Nordic Conference on Human-Computer Interaction* (Oslo, Norway) *(NordiCHI '18)*. Association for Computing Machinery, New York, NY, USA, 473–481. doi:10.1145/3240167.3240174

[26] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't look at me that way! Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 362–372. doi:10.1145/2785830.2785842

[27] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134. doi:10.1016/j.cose.2015.07.002

[28] Tibor Koltay. 2017. *Information Overload in a Data-Intensive World*. Springer International Publishing, Cham, 197–217. doi:10.1007/978-3-319-59090-5_10

[29] Andreas Kotsios. 2015. Privacy in an augmented reality. *International Journal of Law and Information Technology* 23, 2 (03 2015), 157–185. doi:10.1093/ijlit/eav003 arXiv:https://academic.oup.com/ijlit/article-pdf/23/2/157/2062746/eav003.pdf

[30] Sarah M. Lehman and Chiu C. Tan. 2017. PrivacyManager: An access control framework for mobile augmented reality applications. In *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE, New York, NY, USA, 1–9. doi:10.1109/CNS.2017.8228630

[31] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[32] George R. Milne, Mary J. Culnan, and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing* 25, 2 (2006), 238–249. doi:10.1509/jppm.25.2.238

[33] Helen Nissenbaum. 1997. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior* 7, 3 (1997), 207–219. doi:10.1207/s15327019eb0703_3

[34] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Redwood City. doi:10.1515/9780804772891

[35] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (10 2011), 32–48. doi:10.1162/DAED_a_00113 arXiv:https://direct.mit.edu/daed/article-pdf/140/4/32/1830026/daed_a_00113.pdf

[36] 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. doi:10.1080/1369118X.2018.1486870

[37] Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2023. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 6, 4, Article 177 (jan 2023), 35 pages. doi:10.1145/3569501

[38] Robert W. Proctor, M. Athar Ali, and Kim-Phuong L. Vu. 2008. Examining Usability of Web Privacy Policies. *International Journal of Human-Computer Interaction* 24, 3 (2008), 307–328. doi:10.1080/10447310801937999

[39] Halley Profita, Reem Albaghli, Leah Findlater, Paul Jaeger, and Shaun K. Kane. 2016. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4884–4895. doi:10.1145/2858036.2858130

[40] 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

[41] Nisarg Raval, Animesh Srivastava, Kiron Lebeck, Landon Cox, and Ashwin Machanavajjhala. 2014. MarkIt: privacy markers for protecting visual secrets. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (Seattle, Washington) *(UbiComp '14 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 1289–1295. doi:10.1145/2638728.2641707

[42] Holger Regenbrecht, Alistair Knott, Jennifer Ferreira, and Nadia Pantidi. 2024. To See and be Seen—Perceived Ethics and Acceptability of Pervasive Augmented Reality. *IEEE Access* 12 (2024), 32618–32636. doi:10.1109/ACCESS.2024.3366228

[43] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. 2014. Augmented reality: hard problems of law and policy. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (Seattle, Washington) *(UbiComp '14 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 1283–1288. doi:10.1145/2638728.2641709

[44] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (apr 2014), 88–96. doi:10.1145/2580723.2580730

[45] Franziska Roesner, David Molnar, Alexander Moshchuk, Tadayoshi Kohno, and Helen J. Wang. 2014. World-Driven Access Control for Continuous Sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 1169–1181. doi:10.1145/2660267.2660319

[46] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[47] Helen Sharp, Yvonne Rogers, and Jenny Preece. 2019. *Interaction Design: Beyond Human-Computer Interaction* (5th ed.). Wiley. https://www.wiley.com/en-ca/Interaction+Design%3A+Beyond+Human-Computer+Interaction%2C+5th+Edition-p-9781119547259

[48] Jiayu Shu, Rui Zheng, and Pan Hui. 2016. Cardea: Context-aware visual privacy protection from pervasive cameras. *arXiv preprint arXiv:1610.00889* (2016). doi:10.48550/arXiv.1610.00889

[49] Jiayu Shu, Rui Zheng, and Pan Hui. 2017. Your Privacy Is in Your Hand: Interactive Visual Privacy Control with Tags and Gestures. In *Communication Systems and Networks*. Springer International Publishing, Cham, 24–43. doi:10.1007/978-3-319-67235-9_3

[50] Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering Privacy. *IEEE Transactions on Software Engineering* 35, 1 (2009), 67–82. doi:10.1109/TSE.2008.88

[51] Alina Stöver, Sara Hahn, Felix Kretschmer, and Nina Gerber. 2023. Investigating how Users Imagine their Personal Privacy Assistant. *Proceedings on Privacy Enhancing Technologies* 2023, 2 (2023), 384–402. doi:10.56553/popets-2023-0059

[52] Robert Templeman, Mohammed Korayem, David Crandall, and Apu Kapadia. 2014. PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces. In *NDSS '14: Proceedings of the 2014 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, USA. https://www.ndss-symposium.org/wp-content/uploads/2017/09/09_1_1.pdf ISBN 1-891562-35-5.

[53] Sue Wilkinson. 1998. Focus group methodology: a review. *International journal of social research methodology* 1, 3 (1998), 181–203.

[54] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 18 pages. doi:10.1145/3491102.3517688

[55] Tengqi Ye, Brian Moynagh, Rami Albatal, and Cathal Gurrin. 2014. Negative FaceBlurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass. In *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management* (Shanghai, China) *(CIKM '14)*. Association for Computing Machinery, New York, NY, USA, 2036–2038. doi:10.1145/2661829.2661841

[56] Yiqin Zhao, Sheng Wei, and Tian Guo. 2022. Privacy-preserving Reflection Rendering for Augmented Reality. In *Proceedings of the 30th ACM International Conference on Multimedia* (Lisboa, Portugal) *(MM '22)*. Association for Computing Machinery, New York, NY, USA, 2909–2918. doi:10.1145/3503161.3548386

A Appendix

A.1 Focus Groups

A.1.1 Examples for Spontaneous Interactions.

Example 1: Imagine you want to order a coffee from a coffee machine. Today, you would put money into the machine and then press the specific buttons to select the product. That would be an anonymous, manual process. With AR glasses, it could look like you just say through your voice command that you want to order a cappuccino. The systems, vending machine, and your Glass are connected, so your order runs automatically; your charge for the cappuccino is automatically balanced because your financial data has been captured by the AR application. So you only have to take out the end product.

Example 2: Imagine entering the building. It's a smart building that automatically connects to your AR glasses system. The AR glasses have access to your calendar and automatically know what appointment you have today in this building, so they automatically navigate you to the room where your meeting is taking place.

A.1.2 AR Capabilities.

- **Camera Usage:** *"An application generally using the camera(s) on the device"* [37]; Recognition of objects and other people in the environment; Face recognition; Recordings of bystander and of the user's environment.
- **Microphone Usage:** *"An application generally using the microphone(s) on the device"* [37]; Recording of conversations and spatial/ambient sounds; Biometric voice analysis.
- **Volumetric Capture:** *"Capturing 3D imagery that could later be viewed or repurposed (e.g.[,] a 3D model of [one's] body or home)"* [37].
- **Spatial Awareness:** AR systems can understand the physical world around the users through various sensors. This enables objects or information to be accurately placed in the user's environment; Real-time object recognition; Surface detection and mapping; Additional environmental sensors like ambient light sensors or temperature sensors (they can provide context about the user's environment).
- **Activity Tracking:** Monitoring *"the physical movements, [behavior,] and activity"* [37] of the user; Gestural interaction; Head tracking; Body posture and movement tracking; Location tracking.
- **Physiological/Health Monitoring**: *"Understanding the physiological state of [the user], e.g., [capturing] health-related data such as pulse/heart rate, [pupil dilation]"* [37]; Gaze tracking.
- **Diminished Reality:** *"Removing or blocking elements of reality (e.g.[,] ignoring a person"* [37], turning down an environment).
- **Augmented Appearance:** *"Augmenting or altering [the user's] appearance (e.g.[,] applying Snapchat or Instagram-like filters"* [37] to one's profile).
- **Augmented Perception:** *"Canceling noise, selectively enhancing speech in a noisy room; and Supersight or other vision enhancements [(], e.g., zooming, magnification, night/thermal vision[)]"* [37].

A.1.3 Screening Questionnaire.

Demographics.

(1) What is your name? (free text)
(2) What is your e-mail address for contacting you? (free text)
(3) How old are you? (free text)
(4) What gender do you identify with?
  - Male
  - Female
  - Non-binary
  - Prefer not to say
(5) What is your current profession? (free text)
(6) What are you currently studying? If you have already completed your studies, what did you study? (free text)
(7) What is your highest educational qualification? (free text)

Experience.

(1) Have you ever used AR glasses? (yes/no)
(2) Have you engaged with AR/VR applications in the past? (yes/no)
(3) Have you been involved in any hands-on AR/VR projects (development)? (yes/no)
(4) What experience have you already gained with AR/VR? Please describe these in a little more detail. (free text)
(5) How much experience do you have with AR?
  - 0 = no experience
  - Used 1-3 times
  - Used 4-7 times
  - Used more than 7 times

Availability.

(1) Please select all times from the predefined dates when you could participate in the focus group. We will send you the final time slot via email. (Matrix table with listed appointments with the response options "Available" and "Not available")
(2) If none of these times suit you, please suggest all other possible time slots at which you would be available. (free text)
(3) Which languages can you speak?
  - German
  - English

(4) What is your preferred language for the focus group?
- German
- English
- Both languages would work for me

(5) Do you have any further comments? (free text)

A.2 Expert Interviews

A.2.1 *Screening Questionnaire.*

Personal Information and Professional Background.

(1) What is your name? (free text)
(2) What is your e-mail address for contacting you? (free text)
(3) How old are you? (free text)
(4) What gender do you identify with?
- Male
- Female
- Non-binary
- Prefer not to say

(5) Which country do you currently live in? (free text)
(6) In which country were you born? (free text)
(7) What is your highest educational qualification? (free text)
(8) What is your current primary occupation? (free text)
(9) How many years have you been working as a privacy/security expert? (free text)
(10) Do you work in industry or academia?
- Academia
- Industry

Expertise.

(HCI) I am an expert in Human-Computer-Interaction.
- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

(P) I am an expert in privacy domain. (Likert scale)
(SE) I am an expert in security engineering. (Likert scale)
(ID) I am an expert in Interaction Design. (Likert scale)
(AR) I am an expert in Augmented Reality. (Likert scale)
(SHT) I am an expert in Smart Home Technologies. (Likert scale)

Experience.

(EQ1) I am experienced working with privacy-enhancing technologies and mechanisms providing users better control and understanding of their privacy (e.g., privacy dashboards, tangible privacy tools, visualization techniques).
- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

(EQ2) I am experienced in the development of secure system architectures, the establishment of security protocols and frameworks as well as the implementation of data protection and compliance measures. (Likert scale)
(EQ3) I am experienced in developing or designing augmented reality systems (e.g., AR glasses, mobile AR platforms, apps and immersive environments). (Likert scale)
(EQ4) I am experienced in designing user interfaces or interaction experiences (e.g. UI design, UX design, design of interaction flows). (Likert scale)
(EQ5) I am experienced in designing, developing, or analyzing smart home technologies (e.g., IoT devices, home automation systems, user interaction models for smart homes). (Likert scale)

A.3 Expert Interview: Example Scenario

In a futuristic scenario, a customer wearing AR glasses enters a clothing store. The glasses scan the environment and highlight products that match the customer's preferences based on previous purchases. The glasses navigate the customer to the selected product in the store, displaying virtual overlay markers. Interactive 3D product views allow the customer to examine items and information, such as materials or origin, displayed alongside the 3D representation. Using body scan technology, the customer can virtually try on clothes, such as jeans, that are superimposed onto the user's avatar. After selecting products, the user completes the shopping through an automated payment transaction. In addition, delivery of the goods chosen is automatically initiated immediately so that the purchases no longer must be physically carried out.

Figure 10: Generated images to illustrate a speculative future shopping scenario in a clothing store while wearing AR glasses.

While preparing the example scenario, we revised the original scene descriptions using ChatGPT. Further, we developed two corresponding visuals using DALL-E, see 10.