Implications of XR on Privacy, Security and Behaviour: Insights from Experts

Melvin Abraham
m.abraham.1@research.gla.ac.uk
University of Glasgow
Glasgow, United Kingdom

Pejman Saeghe
Pejman.Saeghe@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom

Mark McGill
Mark.McGill@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom

Mohamed Khamis
Mohamed.Khamis@glasgow.ac.uk
University of Glasgow
Glasgow, United Kingdom

ABSTRACT

Extended-Reality (XR) devices are packed with sensors that allow tracking of users (e.g., behaviour, actions, eye-gaze) and their surroundings (e.g., people, places, objects). As a consequence, XR devices pose significant risks to privacy, security, and our ability to understand and influence the behaviour of users - risks that will be amplified by ever-increasing adoption. This necessitates addressing these concerns before XR becomes ubiquitous. We conducted three focus groups with thirteen XR experts from industry and academia interested in XR, security, and privacy, to investigate current and emerging issues relating to security, privacy, and influencing behaviour. We identified issues such as virtual threats leading to physical harm, missing opting-out methods, and amplifying bias through perceptual filters. From the results we establish a collection of prescient challenges relating to security, privacy and behavioural manipulation within XR and present recommendations working towards developing future XR devices that better support security and privacy by default.

CCS CONCEPTS

• **Human-centered computing** → **Mixed / augmented reality**; • **Security and privacy** → **Human and societal aspects of security and privacy**.

KEYWORDS

Augmented Reality, Virtual Reality, Mixed Reality, User-centered security

ACM Reference Format:
Melvin Abraham, Pejman Saeghe, Mark McGill, and Mohamed Khamis. 2022. Implications of XR on Privacy, Security and Behaviour: Insights from Experts. In *Nordic Human-Computer Interaction Conference (NordiCHI '22), October 8–12, 2022, Aarhus, Denmark*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3546155.3546691

NordiCHI '22, October 8–12, 2022, Aarhus, Denmark

1 INTRODUCTION

Extended Reality (XR), referring to both Augmented and Virtual Reality (AR/VR) [40, 53] devices are seeing increasing integration into our daily lives, used in private homes [58], public spaces [20] and more. Driving this adoption are improvements in processing, sensing, form factor, and cost, as we move from headsets that are used frequently throughout the day, towards glasses that may be worn and used all-day (e.g., consumer AR).

XR devices have a large number of sophisticated sensing capabilities to capture their environment, the bystanders that are near the device, and information about the user's actions and physiology. Currently, consumer VR systems such as the Meta Quest, or HTC Vive are the most generally available examples of XR devices. Such VR devices have the capability to capture visual, auditory, and haptic information [3]. These sensors are fundamental for the XR device to function. For example, wide angle camera arrays are necessary to track the position of the Head Mounted Display (HMD) in reality to translate into the virtual environment [7, 12].

The breadth of data available to an XR device amplifies the ability to generate insights from that data. For example, sensitive information can be inferred or estimated (to varying degrees of reliability) [3], such as the user's sexuality [33] or gender [54]. Physical and mental information about the user such as their height can be measured, however more private and serious conditions could potentially be predicted via XR data, such as if the user might develop any illnesses such as Alzheimer's disease [25] or Parkinson's disease [32]. In some cases predicting such personal information about a person is easier when using data from an XR device compared to non XR devices. Examples of this include classifying a user's behavioural traits [8, 24], or emotions [23] in real time.

Due to the nature of the sensors present on XR devices, much more information can be given away than the user or bystanders (who are both physically near the XR user and are not using the device [46]) are potentially aware of [3, 46, 48]. There is a lack of support and effective communication provided to the user, of how their XR data can be processed and analysed.

Even though XR usage is growing, we still have a limited understanding of what security, privacy and behavioural threats are present, or yet to emerge, due to the infancy of the technologies mass adoption. However, even though the security, privacy and behavioural concerns of XR are not fully explored, we still have an understanding of what issues can exist on specific points of the

Reality-Virtuality Spectrum [40]. Literature has considered existing and emergent issues around data access protections [13, 48], privacy concerns [3, 39, 48], and perceptual manipulations [55], and our paper adds to this breadth of consideration around emergent issues. The threats to users' security, privacy, and behaviour need to be addressed preemptively before they are found '*naturally*' and misused '*in the wild*'; otherwise, mass adoption of these devices will enable malicious use-cases.

In this work, we conducted three exploratory expert focus groups, with thirteen experts in total. We recruited experts from both industry and academia that worked in XR, security, and/or privacy. This allowed us to investigate the under-explored, current and emerging issues relating to security, privacy, and influencing user's behaviour in XR.

Prior research such as the work of De Guzman et al. [13] looked at what technical methods exist to protect XR devices. The work by Roesner et al. [48] and Adams et at. [3] looked at a specific boundary within the Milgram et al.'s Reality-Virtuality continuum [40]. Our work looks at devices on the full continuum, to uncover the malicious and harmful uses of user behavioural data collected within XR - a topic that has seen little work within literature. In contrast to prior work which has tended to singularly focus on exploring privacy or security concerns, our work holistically expands our understanding of issues at the intersection of privacy, security, and behaviour manipulation. Through our focus groups, we aim to more broadly explore the unique capacity for XR to both understand, and augment, our activities in reality, and the vulnerabilities and harms this introduces, for instance, around user agency, bystander privacy, identity impersonation and more.

Our results reveal that some users are not aware why and when their data is being collected. Related to this, our experts highlighted their concerns that easily trackable XR data can unveil the user's behaviour and attention, allowing for highly targeted advertisements and influencing user's behaviour. Our findings also indicate a lack of usable Opt-Out/In methods for data collection when using XR. Other issues such as effectiveness of identity theft were discussed along with potential methods to use behavioural information within XR to solve non XR related problems such as user impersonation. Importantly, our experts found a lack of preparedness for mass adoption of XR due to a lack of standards for security, privacy and behavioural data collection and usage.

We discuss the implications of our results, among which, our findings underline the need to develop infrastructures to protect users and bystanders when using or being around XR devices. We also argue that we need to combine our experiences of non XR devices with our current understanding of XR security, privacy and behavioural manipulation to defend against XR threats. Finally, it is necessary to develop human-centric privacy communication methods to allow users and bystanders to exert control over their security and privacy and ensure informed consent.

Our paper specifically contributes a collection of challenges and issues that are currently present or emerging with regards to XR security, privacy and behaviour. We formulate a list of recommendations for future work to create secure and privacy-aware XR systems.

2 RELATED WORK

2.1 Implications of XR Sensing for Users and Bystanders

XR devices are increasingly packed with sophisticated capabilities to sense/capture their environment, proximate bystanders, and the user's actions and physiology. Currently consumer VR systems are the most publicly visible and available example of XR. VR devices have the capability to sense a multitude of information such as, visual, audio, and haptic information [3]. These devices typically support 6DoF positional tracking, which necessitates the inclusion of wide angle camera arrays to track the position of the headset in reality [7, 12].

More information can be given away than the user or bystanders [46] may have been aware of or comfortable with [3, 48]. In addition, the data derived from XR usage can support the inference of unanticipated insights into users and their behaviour [3]. For example disclosing the users sexual preferences [33], emotions [23], and mental state [29]. Other factors such as the users affective state can be estimated [1]; their phenomenological experiences and cognitive processes can be instrumented [22, 26]. XR devices have the sensing capacity to develop comprehensive insights into their users - even when the user assumes the device, or it's sensing capabilities, are not turned on [48]. Leaked raw data from a device such as video, audio, and infrared data can lead a victim uncovering information such as their personality traits [8, 24] which can be used to manipulate the user based on their behaviour, detect a users gender [54], or infer a users cognitive state [11, 16].

As well as uncovering potentially sensitive user information, XR data can also be used to personally identify users. For example, recent research has shown that a user can be personally identified though basic positional data within an VR experience to an accuracy of 90-95% [41, 42].

Risks relating to privacy and security within XR are not only faced by the user of the device but also those around them (i.e., bystanders) [15, 48]. The bystanders of the XR device are at a risk of being sensed, tracked and recorded without their consent or even knowledge [14, 46, 48, 60].

In summary, data that is collected from XR devices can have many implications for both user and bystander privacy. Users may not be aware of the extent of information that can be inferred when data from different XR sensors are combined. The detail of this information allows applications to potentially influence and manipulate their users. Hence, malicious uses of data collection must be further investigated to protect XR users and bystanders. While previous work focused on specific topics within XR privacy and security, our work broadly and holistically assesses the implications of XR sensing on privacy, security and behaviour manipulation through collecting insights from expert focus groups.

2.2 Malicious uses of Extended Reality

Security issues leading to malicious use can create a safety issue resulting in physical harm [55]. A users safety can be at risk if the information rendered to them within their XR device lacks data integrity [13, 48] as users typically assume that displayed content is correct. Thus, a malicious navigation application that

renders incorrect speed limits in front of the speed limit signs [48] could lead to a dangerous environment for both the user and those around them. Similarly a malicious application can harm a user with epilepsy if presented with bright flashing lights [48].

While the previous examples of malicious applications present misinformation or misleading visual effects, XR applications can also potentially alter users' perception of reality in a malicious way. For example, techniques used for redirected walking can lead users to walking into dangerous areas [55].

In summary, there are many security concerns with of XR and a number of emerging threats that are not fully understood. Hence, the threats of a users security must be further investigated to protect XR users and bystanders.

2.3 Communicating Privacy information to Users

XR devices are capable of capturing a breath of information about a user. However privacy protections that are seen on other non XR devices, such as privacy visualisations, data usage awareness, and consent collection are not yet widely adopted within the context of XR and are missing in the literature.

There are many approaches to communicating privacy notices to users [51], such as privacy visualisations [18, 19, 30, 37, 56, 57] or displaying the information as text. Prior Research suggests that that text-based approaches of communicating privacy polices are rarely viewed by the user [59] and contain hard to read legal terms, thus are not a usable solution for the everyday user [4, 17, 28, 30]. Hence to address the usability issues, research has been applied into privacy visualisations, such as methods to communicate privacy attributes to the user.

Privacy labelling exists as a form of privacy visualisation. Their goal is to allow the reader to quickly read and understand the privacy implications of using the device or application [6, 47]. Mehldau proposed displaying icons within categories to in from users of data collection and consequences of the data being collected [37]. Some examples of the categories are "What data?", "How is my data handled?", "For what purpose" and "For how long?". Kelley et al. [30] purposed displaying privacy labels similar to nutrition labels on food packaging. By displaying privacy information in a table, where each row indicates the type of data (e.g., location, cookies, etc) and each column indicates how the data will be used (e.g., profiling, telemarketing). Each cell within in the privacy nutrition label is assigned a visual indicator, "Opt Out" and "Opt In" to display when the data will be collected. It was found when presenting privacy information as labels, the users was able to capture and understand the information faster than if they were to read the same information in a privacy policy [30].

However, one limitation of privacy visualisations are that they all vary in terms of what privacy attributes are communicated to the user [49]. The inconsistencies of the attributes used are due to the lack of standardisation or regulation globally for what privacy information should be displayed to the user. Another limitation of privacy visualisations is they often do not go further than access control, quantity of data collection, and Data Processing attributes [6] thus exclude attributes such as data security or accountability [6].

In summary, there is a lack of lack understanding of privacy and security considerations within XR devices and application. Especially methods of effectively communicate XR privacy and security risks to users that were built specifically for the context of XR, such as immersion or the always on sensors.

2.4 Research Questions

Our work addresses emergent threats and issues through the use of expert focus groups, addressing issues beyond privacy and security of prior work but also the capacity of XR to influence user behaviour. Hence we derive the following research questions for our work, what are the risks and challenges in XR in relation to: RQ1 - data collection and privacy; RQ2 - security; RQ3 - behaviour and influences on behaviour?

3 METHODOLOGY

To explore what issues exist relating to privacy, security and behaviour within the context of XR, three focus groups were conducted with experts in the area. The study was split into two parts: idea generation activities, followed by group discussions. Approval was granted by our institution's Research Ethics Board. Thirteen participants were recruited to take part in the study which took place over video conferencing software, each focus group lasted 75 minutes. Expert focus groups were used to gain insights into security, privacy and behaviour influencing issues within XR. Using experts who have notable experience and knowledge in how XR is evolving and the risks capable with further mass adoption of the technology allowed us to gain multiple perspectives on vast and board topics by participants sharing and developing their ideas together [9, 31].

3.1 Materials and Apparatus

3.1.1 Recruitment. In total three, focus groups were conducted (n = 5, 4, and 4) with 11 participants from Europe and the 2 from the United States of America. For this study the definition of '*expert*' was a person who, if an academic, is at least a senior postgraduate researcher or above, within the areas of extended reality, privacy, and security or, if a practitioner, had at least 5 years of experience working within extended reality. To recruit appropriate participants, we advertised the focus group using online platforms such as LinkedIn, Twitter and at VR4Sec 2021:'1st International Workshop on Security for XR and XR for Security'[1] as well as direct email invitation to those who attended relevant workshops on the topic, connections of the authors, and prominent researchers in the field. In total 17 direct emails were sent, with a response rate of 88.24% (15/17). Out of the 15 people who responded, 13 stated they would like to take part in the study. All the participants who wanted to take part in the study were invited and took part in the focus groups. Participation was completely voluntary, thus no compensation was provided. Each participant filled a basic demographics questionnaire, regarding their XR experience.

3.1.2 Demographic Information. Each participant filled out a pre-participation questionnaire before the focus group asking basic demographics questions, age, gender, and location. The participants

[1] VR4Sec Security for XR and XR for Security https://vr4sec.hcigroup.de/

were then asked to select all the contexts that best suited them, "*I am a researcher in XR*", "*I am a researcher in Security and/or Privacy*","*I work/worked in an XR related company*", and "*I am an XR user*". Finally they were asked "*What XR devices have you used before and for how long (Please use appropriate units)*".

Of the thirteen participants, five were female and eight were male. The option of non-binary and other was available yet was not selected. The participants were within the age range of 24-56 (M = 31, SD = 8.18). Seven participants declared they were exclusively XR researchers, three stated they were exclusively security and/or privacy researchers, and three stated they researched both XR and security and/or privacy. Two of the participants declared they currently work for a company working on extended reality. The participants experiences using XR devices ranged from 1-12 Years (M = 5.17 Years, SD = 3.34).

Focus group one consisted of two participants who stated they researched both XR and security and/or privacy (P4,5), two participants who stated they were exclusively XR researchers (P2,3), and one participant who stated they were exclusively security and/or privacy researcher (P1). None of the participants of this focus group stated they work or worked for a company working on XR. Focus group two consisted of one participant who stated they researched both XR and security and/or privacy (P7), and three participant who stated they were exclusively security and/or privacy researcher (P6,8,9). None of the participants of this focus group stated they were exclusively XR researchers or that they work or worked for a company working on XR. Focus group three consisted of three participants who stated they were exclusively XR researchers (P10,13), one of the three stated they work or worked for a company working on XR (P11). One participant stated they only work or worked at a company working on XR (P12). None of the participants in this focus group stated they research security and/or privacy.

3.1.3 Focus Group Setup. Before the focus group, participants were asked to read an information sheet stating what their participation will entail and how data will be used. The participants then filled out a consent form with options available to ask further questions. The focus group took place using Zoom video conferencing software and Miro for sticky note idea generation. Each participant was assigned a unique ID number which ensured anonymity from the other participants. All the participants changed their display name on Zoom to their ID's then joined the moderator (the lead researcher) within the call. The focus groups were recorded and afterwards transcribed and anonymised.

Five topics were chosen to be discussed in the focus group: Data Collection, Privacy, Security, Behaviour, and Influence. Each topic had prompts to help the participants narrow their responses. These topics were derived from our related work and to aid in answering our research questions.

3.1.4 Miro board Setup. Miro boards[2] are online virtual collaboration tools that represent whiteboards. Three Miro boards were set up with a project, the first board was titled **Data Collection and Privacy**. To help the participants with their answers, some prompts were included: *To what extent are people aware of the data that is being collected in extended reality?*, *What data is collected when using an extended reality device?*, and *What are the privacy issues present?* The second Miro board was titled **Security**, with the prompts *What are the security risks that are present within extended reality.* The third Miro board was titled **Behaviour and Influences**, with the prompts *How aware are users of vendors analysing their behavioral data?*, and *How can behavioral data be used to influence people within XR?* Below the title and pointers, each of the three boards were split into three kanban style sections: *What are the issues within this topic?*, *What are current methods and mitigations to address this approach and your thoughts on this method*, and *What are your thoughts and opinions?* Each focus groups was conducted using new Miro projects, so that the responses were not shared between other groups.

3.1.5 Procedure. **Ideas Generation Activity:** The participants were shown the Miro board titled "*Data Collection and Privacy*" and were given 5 minutes to answer the questions (using the sticky notes feature) within each section (as described in section 3.1.4). While the participants were answering the questions, a timer was displayed. Once 5 minutes were over, the participants were given 2 minutes to read the other responses and add an emoji reaction to sticky notes they agreed with or though were particularly important.

Focus Group Task: After the ideas generation activity (3.1.5), 10 minutes were provided for participants to discuss their responses. A 10-minute timer was displayed to participants during this time. The moderator had minimal involvement besides asking the participants what their thoughts were initially to start the discussion and encouraging equality of participation.

Both the ideas generation activity and focus group task were then repeated for the remaining two Miro boards titled "*Security*" and "*Behavior and Influences*". Once the third focus group task was complete, the participants were debriefed. None of the participants used their right to withdraw from the study at any time.

3.1.6 Limitations. Whilst our results cover only a subset of the potential security, privacy, and influences risks exposed by the adoption of XR, they illustrate novel emergent threats and exemplify the breadth of risks posed. From our findings we present recommendations for creating future XR systems that are privacy and security respecting.

3.1.7 Analysis. The audio from the recorded focus groups were transcribed and anonymised by a researcher. The audio recordings were not translated at any point during the transcription process as they were in English. We used inductive coding [34] to analyse the focus group results and the sticky note tasks in order to develop a qualitative code book. One researcher iteratively coded the data to account for new codes that emerged throughout the coding process. Data from the transcript and sticky note responses were grouped together using codes. The codes were not established prior to the analysis, and emerged through patterns and similar answers within the data. The lead and secondary authors reviewed the final list of codes and grouped together codes with similarities into main themes. This was carried out as a collaborative session where all codes were examined. When reporting the results, the quotes are presented verbatim as they are or they are slightly edited to ease

[2] https://miro.com/

clarity when reading by adding words in square brackets while still maintaining the quote's original meaning.

4 RESULTS

4.1 The Unprecedented Scale and Extent of XR Data Capture

4.1.1 Users are not aware of what XR data is collected, nor the consequences of that collection. A point that was brought up by 4 participants (P11-13) was the HMD's unique capability to pervasively collect data about the users activities, behaviour, physiology, and their bystanders. The users and those around them may not be aware to the extent of the headsets sensing ability and what is done with the collected data. P12 stated "*there's absolutely huge amounts of data [that] can be collected from the you know, the current generation of XR HMD's in general*". P12 then went on to talk about the capabilities of future headsets in collecting data about the headset wearer "*upcoming headsets, like, they're just incredible pieces of technology, and they know huge amounts about user*". P11 also stated that data collection invades the privacy of those around the XR device not only the headset user "*such as recording other people or bystander awareness*"

4.1.2 Users are not aware of when XR data is being collected. Combined with the extensive data collection capabilities XR devices have, the participants (P3,9,10, and 12) stated "*user might not know what data they provide because usually we just consent everything*" (P10). P12 added on to P10 by stating that "*users have very little idea of the amount to date and the types of data that can be that can be collected*" when wearing an XR device.

4.1.3 Users don't realise the value of their XR data. Another point that was mentioned, was on top of how much data is being collected by XR devices, "*users don't generally realize how valuable [their XR] data is*" (P12), referring to the real-time and longitudinal insights that this data could be used to generate both about the user, and the surrounding environment. An example P2 gave, referenced a study that took place,"*a few years ago where they basically could determine the person based on only three characteristics like... gender and where they live and if you now imagine what, for example, AR offers for sensors, I think we all cannot imagine what you can derive from that*".

4.1.4 The necessity of XR data collection. The point of unaware data collection sparked a further discussion of four participants (P2-5) who question why some of the data that is being collected by XR devices is being collected in the first place. The participants stated that there needs to be a clearer difference between data being captured for functionality and data being collected in total, P2 mentioned "*does that data needs to be collected? Or is that for the function of the device? Or is that just because they want it?*". P4 elaborated *We should not at all collect this kind of data for various nonsense applications, if I'm just playing with my HMD, I don't know why is this the kind of data should be used for helping me to shop, or to buy anything*".

A point that was brought up by P12 was about how trustful the public may be to what the protections that are in place, "*Meta & Microsoft have strict controls with respect to 3rd party camera access. That makes sense! But it also makes it necessary for users to trust the HMD providers*".

4.1.5 Capacity for Misinformation. A point that was brought up by the participants (P5-7, and 9) was how incorrect information being presented to a user can create "*threats to a user's safety*" (P5). P7 stated "*altering digital objects and information specially in AR this can not not only be a security concern but also safety concern*", P7 continued to gave an example that "*digital objects and information in user's view can be altered by malicious third-party*". P6 added another example of a person is using a malicious navigation application on their AR headset, "*you say hey please navigate me to the next shop, and then the you are found in a dark ally*".

P6 mentioned how the availability of information is an important factor especially for safety. "*if you are in your house using your HMD, either through malice or literally just in competence or something breaking or failing, a weather alert that would need to be communicated you, it does not get communicated to you, you could be posed to a security risk*". P6 continued to mention that correctness of the information would just as be relevant as availability in causing a user harm "*essentially XR could pose a really big security risk just by giving people the wrong the wrong security cues in certain situations*".

4.2 Access Protections - Facilitating Awareness and Transparency

4.2.1 Users lack an understanding of why their data is needed. Communicating to a user why specific data being collected by the XR device is needed however is not necessarily the solution, as facilitating such awareness brings with it it's own challenges. P1 brought up "*it's quite difficult because people don't understand how the systems work, and if you just tell them, yeah I mean, it needs the data in order to function, they will be happy to offer it, but they don't know that ... we could maybe process the data locally, there's no actual need to share it*". When explaining why information is being collected, visualisation methods fails to communicate the further consequences of the user consent such that P2 stated "*lay users do not know about the consequence of privacy decision*" or present the information in a unusable way such as within a "*license agreement (that nobody reads)*" (P11).

4.2.2 XR headsets should be transparent about data capture and usage. The participants (P3,10,11, and 13) brought up that XR devices and application should communicate to the user when their data is being captured and processed. P3 stated the devices and applications have "*a lot of responsibility of communicating what is there, what are the possibilities, what can be done*" with the users data. P10 mentioned "*transparency is also important here, that the user has to understand what could be the risk while using XR*". P13 went on to comment "*how would you implement or sort of convey this information to users in a usable and understanding way*". P10 and P11 expressed that information regarding what data is being collected and when data collection is occurring, should be presented continuously rather than only at the point of the user giving consent, "*we need info, visual information all the time on the screen, not just at the sign up, so that during the usage of XR device we we will understand what data I'm giving*" (P10). P13 added that when conveying information to the user of when their data is being collected,

the method should not clutter the users view "*providing clear visual cues, how do you do that without cluttering their view, especially if they're using you know AR and potentially need to see elements of the physical environments?*" - emphasizing the trade-off between supporting awareness without overloading the user.

4.3 Cross-Reality Vulnerabilities

Participants also identified vulnerabilities or data exposures in reality (for which the XR user might be unaware) which could then be exploited to harm the XR user.

4.3.1 Identity Theft / Spoofing. Participants (P6,8,10,12) mentioned that there is a higher threat of impersonation and identity theft, as a users stolen XR data being used to recreate their identity within XR. P6 mentioned how collectable the data generated within XR is, "*your movements, gaze and even things you're currently looking at in XR information that you're currently present yourself are very plausibly completely trackable and knowable by someone who has access either corporate or in it, or malicious into your device*".

4.3.2 Physical Safety and Reality Awareness. Four participants (P1,3,5, and 8) mentioned the the dangers and safety concerns of the XR users lack of awareness to what is occurring around them. P3 elaborated "*the person having the headset on in VR like you know they're fully fully immersed in VR you know, they'll be unaware person for somebody nearby a lot of the time right so like that fully aware bystander can take advantage of them*". P3 introduced the idea of a power imbalance between an unaware users and a fully aware bystanders, being used to cause harm "*I noticed from my work we've seen them like, I have instances of bystanders just walking up and pushing them over right*". P8 went further to add there is a need for the user to be alerted about what is happening outside of their immersion "*you're completely isolated and then you don't know what's happening outside so you need some kind of alert to tell you what's happening*".

4.3.3 Security of Virtual and Physical Spaces. Two participants (P2 and 5) brought up that HMD's are now being seen in contexts outside of a private semi controlled location such as at home, "*in the last one or two years, mainly because these VR devices moved out of a home environment like a living room or a lab, really to like a public space*" (P5). The context of where the HMD can change the users acceptance and apply considerations for the devices data collection and security. For example P2 stated "*as a user if I'm just collecting say like my eye movements or something it's like Okay, this is part of the game, but if if I would say, a manager of a project, and we were using a virtual environment to communicate I'd probably be a lot more concerned about how secure this data is*".

4.4 Manipulation of Thoughts, Actions, Behaviour

4.4.1 Sensitivity of Behavioural Data. The participants (P1-9) stated behavioural data captured within XR is highly sensitive and can be used to learn a lot about a user, even in order to influence the user. P9 stated, "*behavioral data is especially sensitive as it can be used to on one hand, learn a lot about the user, of course, but on the other hand, it might also be used to manipulate users*". P5 added how a users behavioural preferences could be used against the user, "*analyse users' preferences e.g., their gaze behaviour to see what color they like most and then present them with items in that specific color to bias them in their purchasing behaviour?*". P11-13 stated behavioural XR data capture could lead to "*novel forms of dark patterns (potentially more subtle/manipulative than non-immersive modalities)*".

Another point brought up was the inclusion of behavioural data collected from XR, being used to expand the different avenues available to observer a user. The participants compared traditional direct interactions tracking that are seen on other devices, to the real time behavioural information collection capabilities of an XR device. An example P6 mentioned was that there were "*far more ways to observe how you interact with media and with the world around you not just your actions directly to a computer interface*". P1,3,4,6, and 7 made a direct link to behavioural data collected from XR being used to facilitate "*targeted advertising*" (P1). P7 went on to say "*they're just basically this shift from advertisement for from advertisement where we had this click through rates and now we have walked through rates*".

4.4.2 Awareness of, and Control over, Use of Behavioural Data. The participants were unclear what the raw XR behavioural data would look like, "*we don't know what the data is going to be like and how much we can use*" (P11). Some of the participants even stated that users are current unaware of why their behavioural data is bring used and who has access to it, P13 asked "*what exactly their data is being used for?*", to which P10 and 12 asked "*will this data be able to be resold?*". Participants 11-3 agreed a method they would be more comfortable with is their behavioural data being processed internally than externally, "*processing as much data as possible on the device* " (P12). P13 questioned how much control a person has over their behavioural data that was collected, "*I think if you do decide to you know delete your data from storage, does that also trickle back to the algorithms that your data is used in to form?*".

4.4.3 Exploiting Behavioural Data. P6 questioned how bias free people generally are and stated the implications of adding another layer of XR behaviour data would lead to "*People are not, I don't think particularly free of heavy influence over the choices, even generally, but I would agree that it's not as if all bad things are the same you know, this is still worse than base advertising*". P6 went on to mention "*Currently companies can observe online interaction behaviour, and even speech behaviours, but with XR comes a whole new array of actions like gaze, how much you interact. Already companies monitor how long one 'lingers' on an advert or video, being able to truly track gaze and attention in this context is scary*".

P5 introduced that the influence a person can face due to their collected XR behaviour data could extend further to outside of the XR device. "*Why do we limit ourselves to within XR? I was more thinking about how can this be used beyond XR in our life, to really have an impact, you know, because the data, you could collect in XR could also be used for any other technology that is not within XR right*".

4.4.4 Perceptual Manipulations. The participants (P5,9, and 10) brought up that there are many techniques within immersive situations that can be used to manipulate a user without them being aware. P10 stated "*there are certain techniques, is able to manipulate you or control you to some degree so we're not, I mean not every user is*

completely aware of being manipulated or agree to be manipulated". Examples of techniques taking advantage of immersion discussed were "*redirected walking*" (P10) and "*shoulder surfing*" (P5,P9).

4.4.5 Trust and Awareness around Manipulations. A point that was brought up by P2-4, P7 and P13 was how little users might be aware they are being manipulated due to their XR behavioural data. P2-4 stated "*potential for a lot more intrusive data collection which may not be obvious to an average user*". P7 commented "*ensuring privacy is one key aspect, because if we don't do it, people can get influenced without their knowledge*". P10 questioned the public opinion of how trust worth and effective the XR device would be when communicating to a user how they should feel about a topic. "*If the technique or the system, the software will tell me, it is a, it is a bad, something it's fake and I wonder whether the user will believe is true or not*".

4.4.6 Benefits of Behavioural Manipulation. P1,2 and 4 discussed some potentially beneficially uses of using behavioural data from XR such as to benefit your physical health. P1 explained "*if a VR applications that you know counts your steps today, and you walk too few steps now, maybe you want to go outside and have walk in the park, I think that's really good if it kind of helps you grow and accomplishing your goals*".

P2 and 4 referred to XR being used as a method to support mental health, "*we can use virtual reality augmented reality to correct some phobias, or some diseases, but it does not replace a real standard protocol of getting cured by some physicians*" (P4). P2 added they have experience using XR devices for immersion therapy, "*I did it for driving hazard perception and number four made good point, it's not the same thing as real life, but if the choices that or nothing then having a sort of middle ground mixed reality environment does help*". P2 went on to describe the phobias they have used XR to help manage "*for fear of public speaking, you had a virtual audience and they either hostile or and gentle when you were speaking*", "*another one was fear of heights*". P4 added "*there is a great advantages of using our own behavior data, behavioural data to do some stuff maybe to help us to speak into a large audience or to help us to I don't know to correct some traumas such we have that occur to us*". However overusing behavioural data was said to be problematic by P1, "*what actually becomes problematic is here when you, you know overuse it and then you kind of have health issues or issues on the social level*".

4.5 Perception of Self and Others

4.5.1 Personal Augmentation. P10 commented about the ability other people may have to add digital content on to their own person, "*Maybe someone can add the digital content above me during an AR scenario*". P10 went on to say, "*that makes me a bit uncomfortable about that, but because I don't know what are you doing to me*", and presented and idea that "*there could be something where every time you need to ask permission for the other person to purchase it to to add additional content above you*". Which P13 responded with, "*I think the idea of asking permission before you I don't know like paste an AR sticker or something to someone else's body, but also for your for your physical spaces*".

4.5.2 Impersonating Others. P11 brought up the topics of XR potentially creating a problem with bots as seen on other social media platforms, "*there is this bot problem right, that I'm not sure if it's going to be bigger or smaller*". It was explained the potential difficulties of developing bots in XR by P11, "*we are reaching to a point that it is getting harder to impersonate a person when you need to recreate an entire person by not by just creating content in a particular sense*". P11 then predicted, "*one of the things with bots, if you manage to have an AI that is a character, that is fully animated, hyper real, like 'this face does not exist' type of thing, it's going to be very hard to tell people that it's not real*". P12 further added a more feasible method to impersonate a person within an XR environment was to "*make an Avatar that looks like another well known avatar you know, maybe impersonate them and use them in a way that that wouldn't be nice*".

4.6 XR as an Amplifier for Existing Vulnerabilities

When developing future XR devices and applications two participants (P10 and 11) brought up that more XR specific security frameworks are needed than bringing in already existing frameworks, that were not built with XR in mind. P10 explained "*The security issue might be different from the from the Web version or a mobile phone version because there's a lot of there's a lot of things to consider in you know an immersive environment*".

An idea that P8 mentioned was that existing security problems that are faced in applications outside of XR might be able to be solved by taking advantage of capabilities found on a an XR device. Security problems such as user impersonation, unauthorised account access due to a compromised password, or unauthorised access to a device used for Multi factor Authentication. "*some stuff like impersonation, for example, it needs a different approach, like behavioural models to make sure that this person is who he or she is actually are*".

4.6.1 Amplifying bias through perceptual filter bubbles. P10-13 discussed that within XR many users can be in the same context however have different experiences. P11 introduced the idea of XR users existing within "*bubbles*", "*this idea that the some people experience very different things, so that they live in the different realities*". P10 stated the problems of bubbles seen within social medias could be heightened within XR, "*in the current social media there are are already many different level and these social bubbles we have and in the XR that could be even more larger*". P10,12,13, added further "*XR filter bubbles could arise in the future (where users experience very different / polarized environments)*".

It was discussed one method to fix the problem of bubbles forming within XR, was with creating consistency within what people are able to see when using their XR devices, "*the idea of sort of consistency is really interesting and I think there may be a lot of contexts where that would be a good solution*" (P13). Consistency in terms of "*you should be able to see what the other person is seeing*" (P11), could lead users to be able to empathise with others "you never know how, seeing thinking from some other people's perspective, I think that that's it's especially relevant for XR".

4.7 A Lack of Preparedness around XR Challenges

4.7.1 Standards and Customisation. During the discussions a point raised was for a "*need of a standard*" (P11). P13 added that "*I agree*

with a need for standards, not only from a privacy side" (P13), P11 went on to add that "*standards for everything such as data collection, security and privacy ... standard with how we can visualise this data, move data, even sharing it*" (P11).

Another issue that was brought up by P10-12, was that XR is missing a usable and clear opt out feature to stop specific data being collected, "*there needs to be clearer opt out*" (P10, P12). P10 continued that applications should be able to adapt to the user opting out specific data, a future opting out mechanism could be implemented similarly to how XR devices handle different levels of immersion, "*I can change the degree of immersion but there's always an opt out option that I can stop everything, I can escape from everything that is being displayed*".

Some of the participants (P1,11,and 13) stated that privacy is not the same for everyone. "*Privacy is highly individual*" (P1), thus when creating privacy guidelines for XR a holistic model would not be appropriate, as P11 states "*specifically with privacy is that the whole idea is that it's contextual*". P13 went on to suggest the difficulties for developers to devise which guideline is appropriate for their use case, "*I feel like a lot of of guidelines are still sort of you know, this is up to your discretion, think about how your users might use this application, but it could vary a lot, so I feel like there's an added challenge of knowing when to apply different guidelines that exist*".

4.7.2 Support for Vulnerable Groups. P11 brought up that there was also lack of safeguarding for specific age demographics and vulnerable groups. "*one thing that I was thinking about was, we are not talking about you know populations at risk, like children right I think that's a particular thing in security, that is not well addressed*". Unique mitigations will likely be needed to support such groups.

4.7.3 Slow Adoption of XR Contributes Towards a Lack of Preparedness. Five of the participants (P6-8,11, and 12) stated that many of the security concerns and issues within XR are still emergent and not-yet fully understood by the research community and industry. P6 stated "*it's such a new technology and [has] a lot of different avenues to explore with how people can exploit the the hardware*" Both P11 and 12 stated "*what harm can a malicious actor inflict on the users, there is definitely a lot more unknowns there*" (P12). P8 went on to add that due to the specific capabilities of XR devices that novel security issues that are to specific XR will arise "*I believe that XR raises a lot of new security concerns that have not been there before*".

P12 made a comparison that as the number of XR users is still relatively small compared to other devices, thus there are more unknowns when it comes to threats. "*just like there was I guess when web services came along and touch interfaces come along there did used to be a lot of unknowns there and I guess if our systems are so small volume you're not a target yet like MAC OSX wasn't a targeted for a very long time as there was nobody using it and windows there was because everyone was using it*".

P13 added that due to the number of unknowns within the area and that the attacks we are aware of are theoretical and never (to our knowledge) have been applied, it will be difficult to convince companies to protect against a specific attack as the attack has never been used in the wild. "*The research community can, you know, investigate all of these possible attacks, and I think some of them might be, really crazy, really maybe unexpected, so I wonder how you then go and convince companies actually prioritize certain tests that we don't have clear evidence that they would ever come up*".

5 DISCUSSION

We discuss the results of our three focus groups and answer our research questions "*what are the risks and challenges in XR in relation to: RQ1 - data collection and privacy; RQ2 - security; RQ3 - behaviour and influences on behaviour?*" by formulating current and emerging challenges within XR. Followed by a list of recommendations and considerations to create secure and privacy protecting future XR devices and applications.

5.1 XR Amplifies Known Challenges – and Exposes Novel, Emerging Vulnerabilities

In reference to RQ2, Our participants brought up that due to the slow adoption of XR devices by society many of the security concerns, risks and capabilities are not yet fully understood. A similar finding is shared by Adams et al [3] where developers stated that one of the reasons for a lack of known and applied malicious uses of XR devices were due to the small size of the VR community.

We have an understanding that is limited by the fact XR, and in particular AR has not yet seen truly mass adoption. Thus there are still significant vulnerabilities and concerns that are yet to emerge. However, even though the security and privacy concerns of XR are not fully understood, we still have an understanding of what issues can exist on specific points of the Reality-Virtuality continuum [40]. Literature has considered existing and emergent issues around data access protections [13, 48], privacy concerns [3, 39, 48], and perceptual manipulations [55], and our paper adds to this breadth of consideration around emergent issues.

In particular our focus group discussed some of the open challenges around XR data collection, regarding trust, necessity, awareness and misinformation and the capacity for cross-reality vulnerabilities due to XR devices. As well exploring XR's unique ability to comprehend, act upon, and influence user behaviour; the capacity for XR to augment perception of self and others and generally the role of XR as an amplifier to existing risks.

Whilst we combine our current knowledge of security and privacy concerns within XR, as well as draw parallels with our experiences with existing frameworks and literature around privacy and security on other devices and applications such as IoT, smartphones, and web apps, we can investigate and build protections for threats before they are found 'in the wild'.

5.2 XR Data Poses Unprecedented Risks

In relation to RQ2 and RQ3 our results show that there is a magnitude of malicious uses for XR and many avenues to cause a person harm within XR. Harm can occur in terms of a persons physical safety as well as a their mental state and behaviours. An example of a malicious use is through the data that is collected when an XR device is used. Data collection from the devices sensors is a fundamental component for the XR device to work, however our participants questioned how much of the data that is being collected is fundamental for the device/application to work, "*does that data needs to be collected? Or is that for the function of the device? Or is that just because they want it?*".

A lot can be learned from the data that is being collected about a user directly such as their height, "*movements*", and "*gaze*" patterns, but also in-directly such as their sexual preferences [33], emotions [23], and mental state. Our participants found that XR allows for such personal information to be accessed easier than compared to capturing the same information on other devices, but also allows for a further capability of long term tracking of personal information. The user should be told from all the streams of data that is being collected, what data collection is necessary for the application to run, and what collection is occurring as an extra. Communicating data collection in such a detail provides accountability and empowers transparency between the user and the application. The user is given the opportunity to decide if they are comfortable using the application.

5.3 The Need for User-Centric Security and Privacy Visualisations

Our participants voiced the need for clearer communication surrounding XR data collection between the user and the XR device or application. P10 commented specifically that users may not be aware of what data they provide. P3 and 10 brought up the need for transparency and explaining to the user what is and can be done with their data.

Rossi and Palmirani stated previously that most privacy visualisation methods fall short due to not being user tested [49]. Hence, XR would benefit with user tested privacy visualisation that communicate what data is being collected, provide a clear explanation for why the data is being collected and how the data will be processed to the user.

Regarding RQ1, P1 argued that, telling the user what data is being collected and that the data is needed for the application to work is not enough. Applications can mislead the user to providing information data by not providing where the data is being processed e.g. locally on the device or on an external server. When communicating about privacy and data collection, the device should also present where the data is being processed, internally on the device or externally.

When presenting security and privacy visualisations to the user, there are a few challenges. P13 pointed out that visual cues should be aware not to clutter the screen of the user, and P10 stated a visual indicator privacy and security should be seen on screen at all time during usage, rather than inform the user during sign up only. A feature seen on iOS devices is that when the camera, microphone or location services are in active use, a coloured dot is presented to the user in the top right of the screen [5]. Similar to most webcams, that also indicate to the user they are in use via a light. Using a coloured dot to communicate to the user data is being captured is not new to XR devices, on an Meta Oculus Quest, a red dot is used to indicate the view of the HMD wearer is being casted, thus other people can see what the user is doing. The Ray-Ban Stories glasses, which are a collaboration with Meta, present that the camera is in use to bystanders by displaying a small white light on the glasses themselves. However, presenting a coloured dot can be easily missed by the user, and also relies on the user to understand which colours represent a specific information stream.

Other methods to convey the same information can be text-based, but text-based info tips were shown to be very ineffective as users do not read the message [59]. Thus XR device users would have a clear understanding of what data is being collected and when, in real time, if on screen security and privacy cues were developed. These communication methods should rely minimally on text, (ideally not at all) to convey information, to not clutter the users view.

5.4 XR Offers the Capacity to Understand and Alter Behaviour - for Better or Worse

XR will facilitate unprecedented understanding of behaviour and actions - in relation to RQ3 this can be used both beneficially and abusively. For example identifying and tracking a user's emotions and mental state via XR data then gradually presenting the user highly emotional content in order to manipulate and bias the user. Alternatively using XR behaviour data for good; as mentioned by our participants XR devices can be an affordable and effective method to work support the users mental health, such as exposure therapy [10]. It's up to both society and academia to ensure the balance falls in favour of benefits, rather than abuses by building protections sooner than later.

With future advances in computer vision, XR devices could allow an entity to track a user's behaviour in real time over a long period of time to predict if the user has/will develop an illness such as Alzheimer's [25] or Parkinson's [32]. Currently health insurance companies already use biometric and health data from smart devices (e.g. a smart watch) to track the health and habits of their customers, such as tracking how many steps the person took today, current and average heart rate, and sleep patterns [36, 45]. Using XR data, from recorded movements to behaviours and actions, health insurance companies can have access to a breadth of additional personal and contextual data that could help model and make predictions, such as the likelihood of developing an illness and expected life expectancy. Such usages of XR data could be both valuable and privacy invasive simultaneously, especially if the user did not fully comprehend the extent to which their data might be (consensually or non-consensually) used, or further insights inferred from it.

5.5 Data from XR and Other Devices Will Lead to More Detailed Privacy Invasive Models of Behaviour

Regarding RQ3, as mentioned data from an XR device allows for a wealth of information to be captured about a person. In addition, when XR data is combined with data from other devices, a highly detailed privacy invasive model of the person can possibly be formed without the users consent of knowledge. For example, as our participants and Mhaidli et al. [38] mentioned, advertisements can become highly targeted using an XR device. P7 brought up that advertisers will now be able to track more about a person using both XR and non-XR devices. Such as combining '*click-though rates*' by logging how many people clicked on a link on a page compared to how many people saw the page on non-XR devices. As well as calculating '*walk through rates*' by tracking rate how many people interacted with a product or shop calculated via image recognition via the users XR device.

5.6 Recommendations Towards Secure and Private XR Systems

In this section, we present a number of recommendations and future work based on the results from our experts to develop secure and private XR devices and applications.

5.6.1 ***Communicate to users when their data is being collected in real time.*** Our first recommendation is that when data is being collected from the user, a visualisation should be provided on screen until the collection has stopped. As mentioned by our participants, due to safety considerations, the visualisation must not obstruct the user's view. Users should also be able to clearly understand where the data that the XR system is collecting is being processed, internally on the device or externally. Finally users should be told what data is being collected when using the application and be presented with how their data will be processed.

These communication methods can help users build a clearer understanding of what is happening to their data, when using their XR device. Presenting information with such transparency can allow developers to both innovate new features and also build trust from by their users [6]. Users can also feel at ease that their data is only being used for the purposes declared [6, 30].

5.6.2 ***Develop applications that can manage variable levels of privacy.*** We recommend that application present a minimum requirement of user data collection that is fundamental for the application to work. In addition to the data collection minimum requirements, a full list of what will be collected should be presented. Allowing user to compare and differentiated the extent of the data they are providing to how much is required for the application to work. When users are able to see such a visualisation, we recommend adding usable methods of opting out/in to specific data collections [50]. Similar altering levels of immersion within current XR devices, such customisation of privacy settings would require developers to build applications that can manage different levels of data availability.

From our experts and research we know that privacy can be a highly personal topic and is different for everyone [43, 44]. Thus allowing for a wide range of user privacy setting customisability and penalisation is in the users best interest [2].

5.6.3 ***XR security, privacy and data standards need to be formed.*** To truly create a secure and private future for XR as a community both academia and industry must collaborate to establish standards for topics such as XR security, privacy, and behavioural data collection. Currently there is work on creating standards for security and privacy within XR [21, 27, 35] but such standards should also have the capacity to address emergent risks such as around behaviour manipulation. Such standards would provide guidance to developers by providing a framework to securely build applications that protect users by default [6]. Users are provided with the assurance that they are protected by knowing how potentially sensitive data such as behaviour collected in XR can be used. In turn preventing users of XR devices form unethical and malicious uses such as behavioural manipulations, for example filter bubbles.

5.6.4 ***Infrastructure is needed to prevent XR impersonation attacks.*** Our findings emphasize that work is imminently needed to prevent user impersonation on XR platforms (e.g. social XR), and using XR devices (e.g. in-person AR identification). One promising approach is the use of continuous verification [52] when wearing an XR device, ensuring that the user wearing the XR device is who they claim they are. If impersonation attacks and avatar cloning cannot be made harder to execute, they risk undermining trust in social XR systems, and further compromising the security of users both in reality and virtuality.

6 CONCLUSION AND FUTURE WORK

In this paper, we explore the emerging challenges that mass adoption of XR will pose regarding three key concerns: security, privacy and influence over behaviour. We present results from three expert focus groups involving participants from both academia and industry reflecting on these concerns. The participants discussed topics such as, XR users not realising how valuable their XR data is when giving apps access, and the amplification of existing vulnerabilities though XR such as impersonations. Based on these challenges, a set of recommendations and future work were provided in support of developing more secure and private XR systems, where key risks, such as behavioural manipulation and over privileged data access, are minimized. In future work it is imperative to address the identified challenges, explore ways to ensure informed consent of data collection without overwhelming users, and support XR applications that allow for users to provide variable data access.

ACKNOWLEDGMENTS

This research is supported by REPHRAIN: The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, under UKRI grant: EP/V011189/1, and by an EPSRC DTP studentship (EP/T517896/1).

REFERENCES

[1] Article 19. 2021. Emotion Recognition Technology Report. https://www.article19.org/emotion-recognition-technology-report/
[2] Fehmi Ben Abdesslem, Tristan Henderson, Sacha Brostoff, and M Angela Sasse. 2011. Context-based personalised settings for mobile location sharing. (2011).
[3] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 427–442.
[4] Annie I Antón, Julia Brande Earp, Qingfeng He, William Stufflebeam, Davide Bolchini, and Carlos Jensen. 2004. Financial privacy policies and the need for standardization. *IEEE Security & privacy* 2, 2 (2004), 36–45.
[5] Apple. 2022. About the orange and green indicators in your iPhone status bar. https://support.apple.com/en-gb/HT211876
[6] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Computing Surveys (CSUR)* 55, 3 (2022), 1–37.
[7] Mitchell Baxter, Anna Bleakley, Justin Edwards, Leigh Clark, Benjamin R Cowan, and Julie R Williamson. 2021. "You, Move There!": Investigating the Impact of Feedback on Voice Control in Virtual Environments. In *CUI 2021-3rd Conference on Conversational User Interfaces*. 1–9.
[8] Shlomo Berkovsky, Ronnie Taib, Irena Koprinska, Eileen Wang, Yucheng Zeng, Jingjie Li, and Sabina Kleitman. 2019. Detecting personality traits using eye-tracking data. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
[9] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. Qualitative HCI research: Going behind the scenes. *Synthesis lectures on human-centered informatics* 9, 1 (2016), 1–115.
[10] Cristina Botella, Javier Fernández-Álvarez, Verónica Guillén, Azucena García-Palacios, and Rosa Baños. 2017. Recent progress in virtual reality exposure therapy for phobias: a systematic review. *Current psychiatry reports* 19, 7 (2017), 1–13.

[11] Andreas Bulling and Thorsten O. Zander. 2014. Cognition-Aware Computing. *IEEE Pervasive Computing* 13, 3 (2014), 80–83. https://doi.org/10.1109/MPRV.2014.42

[12] Shreya Chopra and Frank Maurer. 2020. Evaluating User Preferences for Augmented Reality Interactions with the Internet of Things. In *Proceedings of the International Conference on Advanced Visual Interfaces*. 1–9.

[13] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–37.

[14] 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*. 2377–2386.

[15] Ellysse Dick. 2020. *How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces.* Technical Report. Information Technology and Innovation Foundation. https://itif.org/publications/2020/12/14/how-address-privacy-questions-raised-expansion-augmented-reality-public

[16] Myrthe Faber, Robert Bixler, and Sidney K D'Mello. 2018. An automated behavioral measure of mind wandering during computerized reading. *Behavior Research Methods* 50, 1 (2018), 134–150.

[17] Jan Fernback and Zizi Papacharissi. 2007. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. *New Media & Society* 9, 5 (2007), 715–734.

[18] Simone Fischer-Hübner and Harald Zwingelberg. 2010. UI Prototypes: Policy Administration and Presentation Version 2. http://primelife.ercim.eu/

[19] Grace Fox, Colin Tonge, Theo Lynn, and John Mooney. 2018. Communicating compliance: developing a GDPR privacy label. (2018).

[20] Jan Gugenheimer, Christian Mai, Mark McGill, Julie Williamson, Frank Steinicke, and Ken Perlin. 2019. Challenges using head-mounted displays in shared and social spaces. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–8.

[21] Jassim Happa, Anthony Steed, and Mashhuda Glencross. 2021. Privacy-certification standards for extended-reality devices and services. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 397–398.

[22] Brittan Heller. 2020. Reimagining Reality: Human Rights and Immersive Technology. *Carr Center Discussion Paper Series* 2020-008 (2020).

[23] Steven Hickson, Nick Dufour, Avneesh Sud, Vivek Kwatra, and Irfan Essa. 2019. Eyemotion: Classifying facial expressions in VR using eye-tracking cameras. In *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*. IEEE, 1626–1635.

[24] Sabrina Hoppe, Tobias Loetscher, Stephanie A Morey, and Andreas Bulling. 2018. Eye movements during everyday behavior predict personality traits. *Frontiers in human neuroscience* (2018), 105.

[25] J Thomas Hutton, JA Nagel, and Ruth B Loewenson. 1984. Eye tracking dysfunction in Alzheimer-type dementia. *Neurology* 34, 1 (1984), 99–99.

[26] Marcello Ienca. 2017. Do We Have a Right to Mental Privacy and Cognitive Liberty? https://blogs.scientificamerican.com/observations/do-we-have-a-right-to-mental-privacy-and-cognitive-liberty/

[27] XR Safety Initiative. 2020. The XRSI privacy framework. (2020).

[28] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. 471–478.

[29] Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions.. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems* (Honolulu, Hawaii, USA) *(CHI '20)*. ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3313831.3376840

[30] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

[31] Jenny Kitzinger. 1995. Qualitative research: introducing focus groups. *Bmj* 311, 7000 (1995), 299–302.

[32] Craig A Kuechenmeister, Patrick H Linton, Thelma V Mueller, and Hilton B White. 1977. Eye tracking in relation to age, sex, and illness. *Archives of General Psychiatry* 34, 5 (1977), 578–579.

[33] Daniel J Liebling and Sören Preibusch. 2014. Privacy considerations for a pervasive eye tracking world. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. 1169–1177.

[34] Philipp Mayring. 2014. Qualitative content analysis: theoretical foundation, basic procedures and software solution. (2014).

[35] Mark McGill. 2021. The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy. (2021), 24.

[36] Sam Meenasian. 2015. How Wearable Technology Benefits Health Insurance Companies. https://www.businessinsuranceusa.com/news/technology-related/wearable-technology-benefits-health-insurance-companies/

[37] Matthias Mehldau. 2007. Iconset for data-privacy declarations v0.1,. https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf

[38] Abraham Hani Mhaidli and Florian Schaub. 2021. Identifying manipulative advertising techniques in xr through scenario construction. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[39] Michael Middleton. 2022. The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Business, Finance, and Economics. *The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Business, Finance, and Economics* (March 2022), 1–30.

[40] Paul Milgram, Haruo Takemura, Akira Utsumi, and Fumio Kishino. 1995. Augmented reality: A class of displays on the reality-virtuality continuum. In *Telemanipulator and telepresence technologies*, Vol. 2351. International Society for Optics and Photonics, 282–292.

[41] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 1–10.

[42] Alec G Moore, Ryan P McMahan, Hailiang Dong, and Nicholas Ruozzi. 2021. Personal Identifiability of User Tracking Data During VR Training. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 556–557.

[43] Helen Nissenbaum. 1998. Protecting privacy in an information age: The problem of privacy in public. *Law and philosophy* (1998), 559–596.

[44] Helen Nissenbaum. 2011. A contextual approach to privacy online. *Daedalus* 140, 4 (2011), 32–48.

[45] Parmy Olson. 2014. Wearable Tech Is Plugging Into Health Insurance. https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/?sh=41a80a2d18bd

[46] Joseph O'Hagan, Julie R Williamson, Mark McGill, and Mohamed Khamis. 2021. Safety, Power Imbalances, Ethics and Proxy Sex: Surveying In-The-Wild Interactions Between VR Users and Bystanders. In *2021 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. IEEE, 211–220.

[47] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. Priview–exploring visualisations to support users' privacy awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[48] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and Privacy for Augmented Reality Systems. *Commun. ACM* 57, 4 (apr 2014), 88–96. https://doi.org/10.1145/2580723.2580730

[49] Arianna Rossi and Monica Palmirani. 2017. A Visualization Approach for Adaptive Consent in the European Data Protection Framework. In *2017 Conference for E-Democracy and Open Government (CeDEM)*. 159–170. https://doi.org/10.1109/CeDEM.2017.23

[50] Takahito Sakamoto and Masahiro Matsunaga. 2019. After GDPR, still tracking or not? Understanding opt-out states for online behavioral advertising. In *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 92–99.

[51] 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)*. 1–17.

[52] Terence Sim, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar. 2007. Continuous verification using multimodal biometrics. *IEEE transactions on pattern analysis and machine intelligence* 29, 4 (2007), 687–700.

[53] Maximilian Speicher, Brian D Hall, and Michael Nebeling. 2019. What is mixed reality?. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–15.

[54] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-aware eye tracking using differential privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*. 1–9.

[55] Wen-Jie Tseng, Elise Bonnail, Mark Mcgill, Mohamed Khamis, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. 2022. The Dark Side of Perceptual Manipulations in Virtual Reality. In *CHI Conference on Human Factors in Computing Systems (CHI'22)*.

[56] Bibi Van den Berg and Simone Van der Hof. 2012. What happens to my data? A novel approach to informing users of data processing practices. *First Monday* 17, 7 (2012).

[57] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. 2017. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 5208–5220.

[58] Radu-Daniel Vatavu, Pejman Saeghe, Teresa Chambel, Vinoba Vinayagamoorthy, and Marian F Ursu. 2020. Conceptualizing Augmented Reality Television for the Living Room. In *ACM International Conference on Interactive Media Experiences* (Cornella, Barcelona, Spain) *(IMX '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3391614.3393660

[59] T Franklin Waddell, Joshua R Auriemma, and S Shyam Sundar. 2016. Make it simple, or force users to read? Paraphrased design improves comprehension of end user license agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 5252–5256.

[60] Katrin Wolf, Karola Marky, and Markus Funk. 2018. We should start thinking about privacy implications of sonic input in everyday augmented reality! *Mensch und Computer 2018-Workshopband* (2018).