C. Warin and D. Reinhardt. Vision: Usable Privacy for XR in the Era of the Metaverse. Proceedings of the 2nd European Symposium on Usable Security (EuroUSEC), pp. 111-116. 2022.

Vision: Usable Privacy for XR in the Era of the Metaverse

CHRIS WARIN, University of Göttingen

Institute of Computer Science, Germany

DELPHINE REINHARDT, University of Göttingen

Institute of Computer Science and Campus Institute Data Science, Germany

Extended Reality (XR) — an umbrella term for *Augmented Reality* (AR), *Virtual Reality* (VR) and *Mixed Reality* (MR) — has penetrated the consumer market and is prone to increasingly impact our lives in the near future. Various devices, e.g., MR glasses, AR smartphones apps, or VR headsets, are becoming more affordable, and leader tech companies are heavily investing for a more immersive, realistic, and connected future. Lately, this vision of an interconnected virtual space for people to work, learn, play and share experiences with others has been formulated as the so-called "Metaverse". This expected paradigm shift will heavily rely on XR, and hence implies an unprecedented amount of sensible data being collected about the users. Indeed, XR devices collect large amounts of sensitive data, including biometric data (e.g., eye gaze and body movement data) that are primarily used as *Natural User Interfaces* (NUIs) or for the proper functioning of technologies and services. However, research has identified a number of privacy and security threats rooting from this pervasive data collection, as well as privacy threats regarding XR inputs, outputs, user interactions and devices themselves. Still, further efforts must be made to guarantee the privacy and safety of users in a usable fashion in the future, and XR must be considered as a whole rather than as the sum of its parts to match the vision of the Metaverse. In this context, we propose to analyse the gap between user privacy perceptions in XR as a whole, and their concrete behaviour. The goal of this research is to understand the differences and similarities between AR, MR and VR in terms of user privacy perceptions. This will help us to better understand the relationships between XR variants, which, we argue, is an important requirement to approach the future evolution of these technologies, and to consider usable privacy aspects that match the entire XR spectrum. Adopting this vision early on will be beneficial for future work, and will be the foundation for the implementation of a usable privacy-preserving solution in order to raise awareness and empower users by giving them more control over their privacy in the context of these new and future technologies.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; **Privacy protections**.

Additional Key Words and Phrases: XR, Metaverse, Usable Privacy

ACM Reference Format:

Chris Warin and Delphine Reinhardt. 2022. Vision: Usable Privacy for XR in the Era of the Metaverse. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3549015.3554212

1 INTRODUCTION

XR technologies, including AR platforms (e.g., smartphones), MR glasses (e.g., Microsoft Hololens), and VR headsets (e.g., Meta Quest 2), are progressively becoming mainstream [36, 37, 39]. Over the past decade, XR platforms have

become consumer-ready and affordable, resulting in market size increases and millions of sold devices: the XR market size is estimated to increase from 30.7 billion U.S. dollars in 2021 to 296.9 billion U.S. dollars by 2024 [36]. Furthermore, the amount of XR users has exceeded 135 billion in the US in 2020 [37], and Steam, a video game platform, recorded over 1 million monthly connected VR headsets in 2019 [39].

XR experiences are expected to become more integrated with each other (i.e., through cross-platform applications), more immersive, and to scale to a much bigger extent. Recently, leader tech corporations have formulated this into a term borrowed from science-fiction: the Metaverse. In November 2021, Meta — formerly Facebook — announced the future of the company and its vision for the web, in the form of the Metaverse: An enhanced, interconnected virtual space where users will be able to interact, play, work, learn, and exchange together, through the use of XR [27].

Despite the growing amount of actors investing in this future, there are still doubts about the feasibility of a Metaverse, and doubts about user acceptance. Still, along with Web 3.0, it currently represents the next evolution of the internet, which represents a paradigm shift in terms of human computer interactions, ubiquity, and decentralization. Furthermore, companies such as Meta, Google, and Microsoft are investing billions in technologies and infrastructures that are required to build the Metaverse, especially XR. Thus, regardless of whether this Metaverse trend will fade or not, the future for XR seems stable.

Hence, it seems that the convergence of virtual social networks popularity, XR technologies, and big tech investments will lead to a consequent increase in XR acceptance and usage, and perhaps in the birth of a Metaverse. However, such an environment implies a vast number of concerns for user privacy and security.

First of all, giving an unprecedented amount of sensitive data collected through XR devices and made available to a few data controllers could lead to an exaggeration of already existing problems in our societies. A number of essays [28, 29, 40] point out the inequalities that result from biased Big Data models, which are fed sensitive and/or biased data, and sometimes false data. The outcomes of such models, present at all stages of our societies, end up excluding and hurting women, people of colour, LGBTQ+ communities, and underprivileged communities. Such phenomenons will likely worsen when biometric data will be fed into these algorithms, as Meta intends it with its recent patents for biometric advertising [30]. For example, the analysis of biometric data may reveal sensitive information about the user, such as disability, and could lead to, e.g., discrimination or exclusion [14].

Furthermore, concerns about the Metaverse also stem from its underlying technologies, including XR and blockchain, of which the privacy and security concerns have been analysed in research [11, 44]. However, recommendations have not always been followed, and solutions not always implemented. Today, a number of security features are implemented in XR devices, but privacy-protecting measures are lacking. For example, mobile AR platforms (e.g., Android smartphones), and some VR headsets (e.g., Meta Quest 2, which runs on Android) support access control mechanisms [2], multi-factor authentication [15], and *Software Development Kit*s (SDKs) which implement recognizers (abstraction layers between raw sensor feeds and apps) [3, 16]. In contrast, privacy preserving approaches, e.g. differential privacy for eye tracking, or video sanitization for mobile AR, are not standardised, despite existing solutions in research [11, 32].

In the industry, organizations such as the *XR Safety Initiative* (XRSI) exist, but are scarce. Ground work for standardization of privacy-preserving measures has been laid with the publication of XRSI's privacy framework in 2020 [43]. This includes guidelines for organizations in several domains, such as privacy risk assessment, information, management, and prevention. Still, more work is needed in this direction in order to establish these aspects as industry standards. This includes the adoption or the framework, and technical standards for informed consent as confirmed in XRSI's future roadmap [43]. Indeed, we denote a lack of usable privacy preserving solutions in current XR devices and the need to translate these established guidelines into concrete tools.

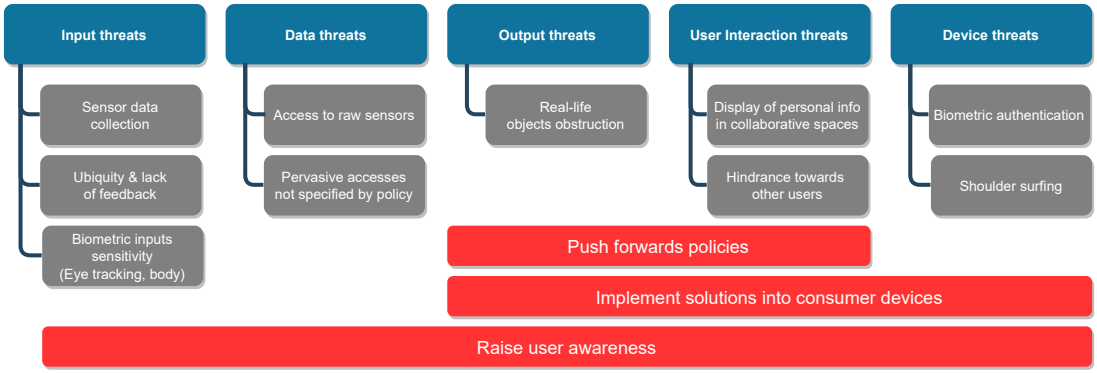

Fig. 1. Overview of privacy threats in XR. Categories are defined in blue, established threats in grey, and current challenges in red.

To address these gaps, we plan to conduct the work detailed in this paper that focuses on usable privacy for XR with a vision matching the Metaverse. In other words, to better understand the privacy risks and the nature of the Metaverse ecosystem, we argue that we need to consider XR as a whole rather than as segmented AR, MR and VR technologies as it has been often done until now when considering privacy. Such global consideration is made possible by recent SDKs and 3D engines that facilitate the development of cross-platform, interconnected experiences across the XR spectrum, which is one aspect of the Metaverse. Thus, our research will rely on cross-platform XR experiences to analyse the existing gaps in usable privacy between the different XR technologies and their combination. With our work, we aim to contribute to the joint efforts of the research field and the industry by giving users the means to easily adapt the different dimensions of their privacy to their individual preferences. For this, we aim to design, implement, and evaluate a usable privacy-preserving solution for XR users.

This vision paper is organized as follows: Sec. 2 expands on the various threats that have been exposed in literature regarding XR. Sec. 3 details usable privacy aspects and links them to our work. Sec. 4 lays out the research questions that we aim to answer over the course of this project, as well as the contributions that we expect to bring to the XR research community. Finally, Sec. 5 concludes this paper.

2 RELATED WORK

There are a number of privacy threats that are being considered regarding the Metaverse. We are currently in the early days of the Metaverse, with only some of its building blocks available. The technology behind it (i.e., blockchain and XR) keeps establishing itself more and more, and improved immersion is on the way. Existing virtual worlds, e.g., Decentraland [12], act as the precursors of the Metaverse, in the sense that they are virtual worlds that replicate real-life aspects, and in which users interact together. They can buy land, clothes, and assets with cryptocurrencies (blockchain-based currencies, e.g. Ethereum). Already, these virtual worlds make extensive use of XR and/or blockchain. The Metaverse represents an evolution of this vision to an even more immersive and interconnected extent, and a much bigger scale. Thus, existing privacy threats in social media, ubiquitous computing, XR and blockchain must be considered for the Metaverse.

Although research on XR has mainly focused on the technology itself and its possibilities, more works with a focus on privacy and/or security have emerged over the years. A 2019 survey by De Guzman et al. has portrayed the state of the art in privacy and security in XR [11]. They gathered and discussed various privacy threats, which they categorized in

five categories, adapting the original classification proposed by Roesner et al. [33]. They categorise privacy and security threats in a data-centric approach, considering input protection, data protection, output protection, user interaction protection, and device protection, as shown in Figure 1. However, usable privacy aspects are not considered.

2.1 Input threats

Threats to inputs can be categorized for passive and active inputs [11]. Threats to passive inputs essentially root from the large amount of information gathered by the sensors of XR devices. This notably includes cameras, which can detect objects in the environment of users and bystanders [1, 13, 20]. Moreover, research has been conducted on privacy threats regarding spatial data, which is necessary for the functioning of XR. AR and MR devices use gyroscopes, accelerometers, and cameras to detect planes and anchor virtual content on top of the perceived reality. Recent works demonstrate the risks of spacial inference attacks (i.e., identification of a given space using a 3D spacial map) [9, 10, 25]. Another concern lies in the ubiquitous nature of XR devices and their lack of feedback regarding data collection. Users do not easily know whether embedded cameras and microphones are recording or not [1, 41].

Active inputs given to XR devices notably include eye gaze and hand/body gestures, which have been shown to be sensitive data. Eye tracking could for example be used to identify user interests, based on fixation time and pupil size [38], or to identify users [8]. Body gestures have also been shown to be sensitive data which can identify users. Miller et al. analysed the tracking data from 511 participants that watched immersive videos with a VR headset and were able to identify the users from the tracking data with 95% accuracy [26]. A 2021 study was conducted over two sessions, to observe the possibility of re-identification across several days [24]. The authors found that their model could personally re-identify participants with a 90% accuracy. Although this could be beneficial for implicit authentication, this also represents a privacy risk for users, who could be identified through the tracking of their behaviour and movements. Although these privacy threats have been established, there is, to the best of our knowledge, little to no user awareness regarding the sensitivity of their biometric data, which shows the importance of implementing usable privacy standards in XR devices in order to mitigate this.

2.2 Data threats

Because of the high amount of data gathered by the sensors embedded in XR devices, there is a risk of data leaking to, e.g., third parties [11]. Research has advocated for the use of abstraction layers between raw sensors and applications to prevent access to raw sensor feeds, e.g. the entire camera feed of the device [7, 20]. Although this is nowadays an industry standard (e.g., mobile AR SDKs such as Google ARCore provide recognizers to developers to facilitate augmented content), recent work has shown that applications can still make pervasive accesses (i.e. not specified in the associated privacy policy) to sensors in both active and passive use of mobile AR applications [18]. Furthermore, Lehman et al. demonstrated the possibility to get camera frames access with Google ARCore [23], which is used by more than a billion Android users [17]. To avoid third parties leaking personal info, it is therefore crucial to secure data collection, data processing, and data storage, even more so in the context of the Metaverse. Furthermore, it is important to raise user awareness regarding data leaks, as a better understanding of the stakes at risk may discourage some to disclose personal data in certain contexts, thus reducing the amount of attack vectors for adversaries.

2.3 Output threats

AR and MR devices are outputting augmented content to the user, and more devices – e.g., the Microsoft Hololens – support multi-application ecosystems, with potentially multiple applications displaying content simultaneously [33].

However, there are little to none output access control systems in current devices. Thus, adversaries could compromise user safety by hiding real life important information (e.g., a stop sign) by overlapping augmented content over the user's vision, or over other applications' output [32, 33]. To mitigate this, Lebeck et al. proposed an AR output access control framework that displays content depending on the specified policies [21]. Still, such solutions will need to be ported over to consumer devices in the future, in order to let users control the amount of output and intrusiveness of XR apps, through clear and understandable policies.

2.4 User interaction threats

XR experiences in the Metaverse are meant to be increasingly more collaborative and interactive. As such, in order to preserve users' privacy, sensitive user content needs to be displayed accordingly in collaborative spaces (i.e., should be shown only to authorised parties to maintain confidentiality) [33]. Furthermore, malicious users have to be considered, especially given the existing cases of user hindrance towards other users (e.g., virtual vandalism, personal space invasion) [32, 34]. Lebeck et al. gathered user perceptions regarding privacy and security for multi-user AR experiences, which notably included concerns about physiological attacks, deception, inappropriate content, and advertisements [22]. This lays ground work in understanding the impact of group dynamics in user privacy concerns, which has been discussed in previous reviews about information privacy [4, 35]. Raising awareness, pushing forward policies, and proposing solutions adapted to the users' characteristics is required to mitigate these concerns.

2.5 Device threats

In order to ensure the privacy protection of inputs, outputs, data and user interactions, XR devices also need protection regarding device access and physical interfaces [11]. User authentication can be verified through novel methods, such as behavioural biometric user identification [24], as mentioned earlier, although the behavioural tracking data is sensible and can be at risk. Moreover, the disclosure of personal augmented output through, e.g., shoulder surfing (i.e., the ability of a bystander to observe a user's personal content by standing behind them), has to be considered. Here, optical strategies, such as glass polarisation, and visual cryptography, are possible leads [11]. Threats to physical interfaces will likely expand in the future, with more interconnected experiences with different devices, leading to an increase in usage and thus, more situations endangering user privacy.

3 USABLE PRIVACY FOR XR

Because we are currently molding XR to become more accepted and streamlined in the perspective of the Metaverse, it is capital to understand how users will behave with the future iterations of these technologies, especially in terms of privacy, and hence to consider usable privacy aspects while we are still in this phase.

We have previously identified gaps and challenges in the field of privacy in XR, which mostly include the lack of user awareness regarding the sensitivity of their data and the nature and volume of data collection, the need of implementing more (native) privacy mechanisms in XR devices, and the need for clear and understandable policies to be up to date in terms of legality, morality and ethics [11]. However, the evolution towards the Metaverse implies more interconnectivity between XR devices, meaning an increase in different devices, vendors, and interfaces. This represents a challenge for enforcing native privacy preserving solutions.

Thus, to mitigate the open gaps in the field with an up to date vision, we need to design studies and solutions to: 1) understand user privacy perceptions regarding XR and the Metaverse; 2) understand the stakes for the technologies to come; 3) enforce user privacy requirements. These design considerations can be seen through different lenses. Wong

and Mulligan [42] describe different dimensions of design practices that relate to privacy, and how design serves privacy in published research. Our intended work will first use design "To Explore People and Situations" [42]: To provide users with means to better protect their privacy, we first need to understand their perceptions and behaviours by designing situations that highlight privacy aspects while experimenting XR, in the scope of a lab study. Then, we will use design "To Inform or Support Privacy" [42], with tools to enforce the privacy requirements that we will have learnt about previously. These design purposes fall into user-centered design.

Following this user-centered vision, we may consider the steps users encounter when using XR, to better assist them throughout their XR experiences. This can notably include: 1) installing and registering for an application, requiring the acceptance of privacy policies; 2) the authorisation of requested accesses to resources for, e.g., third parties, through privacy notices; 3) using the app with an expectation for transparent data collection; 4) interacting safely with other users in-app and in real-life; 5) accessing the collected data in an easy way; 6) revoking access rights and/or uninstalling an application. Our work will consider such scenarios so that usable privacy aspects are embedded at as many steps of users' experiences as possible.

4 RESEARCH QUESTIONS AND EXPECTED CONTRIBUTIONS

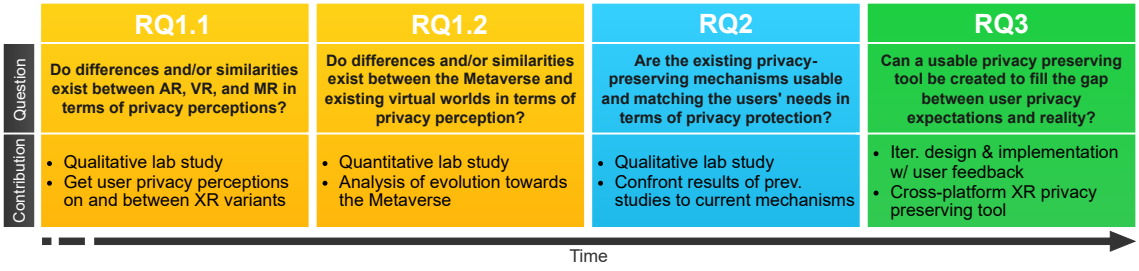

Fig. 2. Our research plan with research questions, and expected contributions.

Our specific research plan, as well as our expected contributions, are outlined in Figure 2. The goal of our work is to provide XR users with a privacy preserving tool to mitigate the privacy threats that we previously cited. This solution may further be extended in future work, and become ground work for cross-platform XR privacy tools. We are expecting to contribute 1-2 papers for each of our research questions, which we discuss in the following.

Our research will first investigate the existing awareness, concerns and expectations of users around XR technology, and measure the extent of the gap between these considerations and the concrete behaviour of users with XR devices in their current form, but also in expectation of their future evolution. These considerations will likely fall in the input threats category of the taxonomy shown in Figure 1, as hinted by the considerations of users when facing AR technology as shown in a 2014 study [13]. In order to define a scope for our initial research, we shall also consider data threats aspects in the design of our studies, as there is a logical link between what data is collected, and how, when, and by whom this data is accessed. Hence, we can formulate **RQ1**: *What are users' privacy perceptions on the current XR technology and future Metaverse?* This considers multiple aspects, including privacy perceptions over the entire XR spectrum, as well as a temporal dimension of current versus future technology. Thus, we may subdivide these aspects into two research questions.

RQ1.1: *Do differences and/or similarities exist between AR, VR, and MR in terms of privacy perceptions?* Existing XR research has mostly been segmented to one or two dimensions at a time (i.e., either concentrated on VR or AR/MR) rather than approaching XR as a whole. The comparison of the technologies will allow us to understand the way they interface together, and what privacy aspects and threats emerge from the interconnectivity between different XR devices. The consideration of this interconnectivity, i.e., cross-platform applications, SDKs, and tools, matches the vision of the Metaverse. We argue that adopting this vision early on allows for a better perception of potential future experiences, and hence, facilitates the design of usable, durable, and relevant privacy solutions for the future while the technology is still maturing. With this global vision in mind, we will conduct a first qualitative lab study to observe user behaviour and user privacy perceptions on XR. For this, we will develop a cross-platform XR application that will be compatible across mobile AR (with an Android smartphone), MR (Microsoft Hololens), and VR (Meta Quest 2), by using Unity 3D which supports all three platforms. We will compare the differences in terms of privacy perceptions using all three variants of the XR applications, which will help answer the research question. The development of this cross-platform application will be done with Unity3D, an engine which supports all three XR devices. It will allow us to investigate differences in privacy perceptions for the same application, but with different devices.

RQ1.2: *Do differences and/or similarities exist between the Metaverse and existing virtual worlds like VRChat, AltSpaceVR and Horizon Worlds in terms of privacy perception?* With this question, we seek to observe the evolution between the existing premises of the Metaverse and its expected future outcome, with respect to privacy aspects. This analysis may include considerations such as the (expected) amount of data collection, the way that users will interface with XR devices, and the proposed mechanisms to guarantee user safety. For this, a quantitative user study will be conducted to gather user expectations of existing virtual worlds such as VRChat or AltSpaceVR, and their expectations of the Metaverse. This study will contribute to better understand the current and upcoming stakes of virtual social networks from a user-centric perspective.

These studies will lay the groundwork needed to identify and prioritise user privacy perceptions and privacy requirements for XR. We will then confront these considerations against the existing privacy-preserving mechanisms in current XR devices and/or experiences. This is mandatory to observe the current solutions and their shortcomings in order to develop a usable solution that will aim to fill this gap. This yields **RQ2**: *Are the existing privacy-preserving mechanisms usable and matching the users' needs in terms of privacy protection?* A lab study will determine whether the existing mechanisms match users' privacy perceptions in XR experiences as observed in RQ1.

The output of RQ1 and RQ2 will be fed into **RQ3**: *Can a usable privacy preserving tool be created to fill the gap between user privacy expectations and reality?* As such, the results of the user studies will serve as foundation for the design of a usable privacy-preserving solution for XR devices. Although the nature of this solution is yet unclear, we are considering a cross-platform tool to enable the protection of privacy aspects that are common to all XR variants, but also privacy aspects that are specific to each variant of the XR spectrum. A unique solution for all platforms, but that still tailors the available privacy settings for the platform on which it is installed, will provide more learnability, efficiency and memorability for users (through the provided sense of familiarity given by, e.g., similar user interfaces for all variants), while preventing them from having to adapt to each solution individually. These quality components define usability [19], and are therefore critical aspects to incorporate in the design of a usable privacy preserving solution.

The design and implementation of this solution shall be iterative in order to include user feedback and further ensure its usability. For this, several lab studies will be conducted to observe users' interactions with the solution, and their feedback will be gathered through, e.g., a *System Usability Scale* (SUS) questionnaire [6]. With this work, we aim to: (1) Allow users to have a usable solution to better protect their privacy; (2) Contribute to a fairer, more transparent and

respectful virtual ecosystem for users; (3) map a bridge between existing research and industry standards and practices. This could increase the acceptance and adoption of XR technologies.

Additionally, our privacy-preserving solution will give users more control over their privacy in these new digital ecosystems. However, it has been shown that giving more control to users over their privacy results in the so-called privacy paradox, where users perceiving more control over their data may disclose more personal information than users who do not perceive control over their privacy [5]. Hence, a balance between user effort, control, usability and privacy must be found [31].

5 CONCLUSION

The rise in availability, affordability and popularity of XR devices, coupled with the fast progression towards the Metaverse, pushes forward the importance of protecting the privacy of users in the context of these new technologies. The increased amount of personal data given through XR devices increases the risks of privacy breaches, which could be even more devastating in a Metaverse, given the negative impact that big data can already have today. Because the Metaverse will be facilitated by XR technology, we seek to observe user perceptions on current and future technology to observe the gap between privacy expectations and behaviours. The novelty of our approach lies in the consideration on XR as a whole rather as the sum of segmented domains, which are often not considered together. This vision matches the idea of the interconnected experiences that the Metaverse represents and may help finding new privacy threats regarding cross-platform XR experiences. We plan on conducting several studies in order to 1) observe user privacy perceptions on cross-platform XR apps, 2) understand similarities and differences between existing virtual worlds and the Metaverse, and 3) determine whether the existing privacy preserving measures in current XR devices and experiences match the privacy requirements of users. The result of these studies will serve to design a usable privacy enhancing solution to empower users and raise their awareness.

REFERENCES

[1] 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 *Proc. of the 14th USENIX Symposium on Usable Privacy and Security (SOUPS)*.

[2] Android. 2022. Permissions on Android. Online: https://developer.android.com/guide/topics/permissions/overview (accessed in 6.22).

[3] Apple. 2022. ARKit 6 – Augmented Reality – Apple Developer. Online: https://developer.apple.com/augmented-reality/arkit/ (accessed in 6.22).

[4] France Bélanger and Robert E Crossler. 2011. Privacy in the Digital Age: a Review of Information Privacy Research in Information Systems. *MIS quarterly* (2011), 1017–1041.

[5] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* (2013).

[6] John Brooke. 1996. SUS: A "Quick and Dirty" Usability Scale. *Usability Evaluation in Industry* (1996).

[7] Loris D'Antoni, Alan Dunn, Suman Jana, Tadayoshi Kohno, Benjamin Livshits, David Molnar, Alexander Moshchuk, Eyal Ofek, Franziska Roesner, Scott Saponas, Margus Veanes, and Helen J. Wang. 2013. Operating System Support for Augmented Reality Applications. In *Proc. of the 14th Workshop on Hot Topics in Operating Systems (HotOS XIV)*.

[8] Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. 2021. A Privacy-preserving Approach to Streaming Eye-tracking Data. *IEEE Transactions on Visualization and Computer Graphics* (2021).

[9] Jaybie A. de Guzman, Aruna Seneviratne, and Kanchana Thilakarathna. 2021. Unravelling Spatial Privacy Risks of Mobile Mixed Reality Data. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* (2021).

[10] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. A First Look into Privacy Leakage in 3D Mixed Reality Data. In *Proc. of the 24th European Symposium on Research in Computer Security (ESORICS)*.

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

[12] Decentraland. 2022. Welcome to Decentraland. Online: https://decentraland.org/ (accessed in 6.22).

[13] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies. In *Proc. of the 33th SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[14] Ben Egliston and Marcus Carter. 2021. Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse. *Internet Policy Review* (2021).

[15] Facebook. 2022. What is Two-factor Authentication and how does it Work on Facebook? Online: https://www.facebook.com/help/148233965247823/ (accessed in 6.22).

[16] Google. 2022. ARCore. Online: https://developers.google.com/ar (accessed in 6.22).

[17] Google. 2022. Google Play Services for AR. Online: https://play.google.com/store/apps/details?id=com.google.ar.core (accessed in 6.22).

[18] David Harborth, Majid Hatamian, Welderufael B Tesfay, and Kai Rannenberg. 2019. A Two-pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality applications. In *Proc. of the 52nd Hawaii International Conference on System Sciences (HICSS)*.

[19] Jakob Nielsen. 2012. Usability 101: Introduction to Usability. Online: https://www.nngroup.com/articles/usability-101-introduction-to-usability/ (accessed in 6.22).

[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 *Proc. of the 22nd USENIX Security Symposium (USENIX Security)*.

[21] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2017. Securing Augmented Reality Output. In *Proc. of the 37th IEEE Symposium on Security and Privacy (S&P)*.

[22] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End users. In *Proc. of the 38th IEEE Symposium on Security and Privacy (S&P)*.

[23] Sarah M Lehman, Abrar S Alrumayh, Haibin Ling, and Chiu C Tan. 2020. Stealthy Privacy Attacks against Mobile AR Apps. In *Proc. of the 8th IEEE Conference on Communications and Network Security (CNS)*.

[24] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In *Proc. of the 40th SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[25] Hongbin Liu, Jinyuan Jia, and Neil Zhenqiang Gong. 2021. PointGuard: Provably Robust 3D Point Cloud Classification. In *Proc. of the 34th IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.

[26] 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* (2020).

[27] Stylianos Mystakidis. 2022. Metaverse. *Encyclopedia* (2022).

[28] Cathy O'Neil. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* Broadway Books.

[29] Caroline Criado Perez. 2019. *Invisible Women: Data Bias in a World Designed for Men.* Abrams.

[30] Financial Post. 2022. Facebook Patents Reveal how it Intends to Cash in on Metaverse. Online: https://financialpost.com/fp-finance/facebook-patents-reveal-how-it-intends-to-cash-in-on-metaverse (accessed in 6.22).

[31] Christian Reuter, Luigi Lo Iacono, and Alexander Benlian. 2022. A Quarter Century of Usable Security and Privacy Research: Transparency, Tailorability, and the Road Ahead. *Behaviour & Information Technology* (2022).

[32] Franziska Roesner and Tadayoshi Kohno. 2021. Security and Privacy for Augmented Reality: Our 10-Year Retrospective. In *Proc. of the 1st International Workshop on Security for XR and XR for Security (VR4Sec)*.

[33] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and Privacy for Augmented Reality Systems. *Commun. ACM* (2014).

[34] Ruth, Kimberly and Kohno, Tadayoshi and Roesner, Franziska. 2019. Secure Multi-User Content Sharing for Augmented Reality Applications. In *Proc. of the 28th USENIX Security Symposium (USENIX Security)*.

[35] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: an Interdisciplinary Review. *MIS quarterly* (2011), 989–1015.

[36] Statista. 2021. Augmented (AR), Virtual Reality (VR), and Mixed reality (MR) market size 2021-2024. Online: https://www.statista.com/study/29689/virtual-reality-vr-statista-dossier/ (accessed in 6.22).

[37] Statista. 2022. Extended reality (XR): AR, VR, and MR in the United States. Online: https://www.statista.com/study/86679/extended-reality-xr-ar-vr-and-mr-in-the-us/ (accessed in 6.22).

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

[39] Road To VR. 2019. Analysis: Monthly-connected VR Headsets on Steam Pass 1 Million Milestone. Online: https://www.roadtovr.com/monthly-connected-vr-headsets-steam-1-million-milestone/ (accessed in 6.22).

[40] Sara Wachter-Boettcher. 2017. *Technically Wrong: Sexist Apps, biased Algorithms, and other Threats of Toxic Tech.* WW Norton & Company.

[41] Katrin Wolf, Karola Marky, and Markus Funk. 2018. We should start thinking about Privacy Implications of Sonic Input in Everyday Augmented Reality!. In *Proc. of the 17th GI Conference on Mensch und Computer*.

[42] Richmond Y Wong and Deirdre K Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proc. of the 38th SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[43] XR Safety Initiative. 2020. The XRSI Privacy Framework. Online: https://xrsi.org/publication/the-xrsi-privacy-framework (accessed in 6.22).

[44] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. *ACM Computing Surveys (CSUR)* (2019).