EUI ROBERT SCHUMAN CENTRE

RSC 2023/69
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

Eye-tracking devices for virtual and augmented reality Metaverse environments and their compatibility with the European Union General Data Protection Regulation

Natalia Menéndez González and Efe Bozkir

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

Eye-tracking devices for virtual and augmented reality Metaverse environments and their compatibility with the European Union General Data Protection Regulation

Natalia Menéndez González and Efe Bozkir

RSC Working Paper 2023/69

ISSN 1028-3625

Published in December 2023 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

Views expressed in this publication reflect the opinion of individual author(s) and not those of the European University Institute.

With the support of the
Erasmus+ Programme
of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The EUI and the RSC are not responsible for the opinion expressed by the author(s).

Centre for a Digital Society (CDS)

The Centre for a Digital Society (CDS) was created in 2022 and is directed by Prof. Pier Luigi Parcu. It analyses the chal-lenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Robert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims to advise policy makers on how to cope with the challenges that are generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach, relying on in-house expertise in law, economics and political sciences, and by actively cooperating with computer scientists and engineers from partner institutions.

For further information: https:// digitalsociety.eui.eu

Abstract

Even though the Metaverse from science fiction is not a reality yet, it is possible to take a glimpse into how it might look like. Several companies and platforms are currently working and developing their versions of how the Metaverse will look in a not-so-distant future. However, the current vision of the Metaverse does not only encompass software. A great deal of companies is complementing their Metaverse projects with Virtual and Augmented Reality devices such as headsets and glasses. In this line, one of the last technological advancements in virtual and augmented reality devices included the introduction of eye-tracking technology. However, when new and additional kinds of data are processed, emerging risks for data protection might arise. While there is an already incipient stream of scholarship that analyses the risks that eye-tracking devices might entail for privacy, such literature mostly focuses on the technical side. However, no scholarship, up to this moment, has examined such devices from a legal perspective and particularly from a data protection lens. This paper will, therefore, discuss the compatibility of eye-tracking devices for virtual and augmented reality environments with the European Union General Data Protection Regulation (GDPR). Being the GDPR considered a worldwide role model in terms of fundamental rights protection, the compatibility of such devices with one of the most severe data protection regimes will be put to the hardest test. The paper will do so by analyzing the state of the art of the technology, its use in headsets and glasses for virtual and augmented reality Metaverse environments, and the potential risks that such use might entail for data protection. After that, such risks will be confronted with the relevant applicable provisions of the GDPR. Finally, the paper will issue policy recommendations regarding the need for more interdisciplinary research on privacy-enhancing techniques to solve the privacy-utility conundrum; careful monitoring of access to data by third parties, including data security and minimization requirements; more guidance from supranational Data Protection Authorities and more attention when designing privacy policies, especially for children.

Keywords

Metaverse; Virtual Reality; Augmented Reality; Eye Tracking; GDPR

Table of contents

1. Introduction

The Metaverse was born in science fiction and has ended up becoming a reality. The term was first used by Neil Stephenson in his 1992 novel Snow Crash, and it represented 'the vision of escaping to a place where digital displaced the physical' (Levi, 2022). This is exactly the idea behind the current development of the Metaverse: to be able to do all the things humans can do within the physical world but in virtual environments and many more, some of them perhaps unimaginable nowadays. Even though the Metaverse is not yet a mature technology, it has been widely reportedly used in fields with high social relevance such as healthcare (Marr, 2022) and education (Cortés, 2022).

The Metaverse experience requires an entrance door. It is not possible to fully immerse into its wonders with a computer, a tablet, or a mobile phone, for instance. For new worlds, new tools are needed to make the most out of them. To accomplish this task, different hardware solutions have been developed such as Augmented Reality (AR) glasses or Virtual Reality (VR) headsets. To further make the experience even smoother, state-of-the-art VR and AR devices are starting to increasingly incorporate eye-tracking technology. Such technology allows mimicking the person's facial expressions with their virtual avatar or providing better image quality and performance. In addition, it helps users interact with the visualizations and spaces in a hands-free way (Lystbæk and others, 2022) and personalize the content based on users' behaviors (Plopski and others, 2022).

With increasingly more complex and modern technologies, the challenges surrounding such technologies also get more complex. From a legal perspective, the addition of eye-tracking technology, apart from a great deal of new functionalities, also entails a new set of risks. More specifically, from a privacy and data protection point of view, the use of eye-tracking technology entails an additional amount of data gathered and processed, eye-tracking data, which, in some cases, might be personal data.

This study is the first to focus on the specific legal implications of the use of eye-tracking technology in VR and AR devices for Metaverse environments. Previous studies (Agencia Española de Protección de Datos, 2022; Bolognini, 2022; Cerrina Feroni, 2023) have identified various ethical and legal risks of the Metaverse, but their engagement with eye tracking is limited or inexistent. The scarce literature digging into the (mostly) privacy implications of the use of eye tracking in VR and AR has a strong technical approach (Bozkir and others, 2023; Kröger and others, 2020). While this approach is necessary for data protection by design and default[1] purposes, it is not enough. Therefore, this paper will look at the impact of eye-tracking technology within VR headsets for Metaverse environments from a data protection lens. It will also discuss the compatibility of eye-tracking devices in AR/VR for Metaverse experiences with the European Union (EU) data protection regulation. More specifically, the paper will analyze their compatibility with the EU General Data Protection Regulation (hereinafter, GDPR). Being the GDPR considered a worldwide role model (Bradford, 2019) in terms of fundamental rights protection, the data protection compliance of such technologies will be put to the hardest test.

This paper is structured in five parts. Part one has introduced the context and justification of the research. Part two will outline the privacy and data protection risks of eye-tracking technologies. Part three will dig deeper into the privacy policies of several VR and AR devices and their compatibility with the legal framework of the GDPR. Part four will point out some policy recommendations regarding the challenges discussed within parts two and three and part five will summarise the conclusions of the paper.

[1] See Article 25 GDPR.

2. Privacy and data protection risks of eye-tracking technology

Eye-tracking hardware and software technologies obtain and process eye-tracking data which consists of ‘eye movements and eye positions of an individual’ (Lim, 2022). To process eye-tracking data, VR devices first capture an image of the eye. This image will constitute the raw data that, as it will be further explained, is often not processed by eye-tracking providers due to privacy reasons. After that, a mathematical algorithm is applied to estimate the gazing direction. The European Data Protection Board has established that as long as the biometric characteristics are captured to be transformed for comparison purposes, they should be considered personal data.[2] It should be considered that the European Court of Justice contemplates a very broad definition of what is personal data, applying it even to IP addresses.[3]

Such information will be considered personal data (and thus subject to the GDPR) if an individual can be identified or identifiable through it or if personal characteristics can be inferred from them. There are various ways through which eye-tracking data can fall into this definition. In some cases, the goal of eye-tracking is precisely to collect personal information about individuals. In others, the collected data is not gathered with that goal, but it nonetheless can be reused to make inferences about individuals. Either way, the resulting data is classified as personal data under European Union Law.

When personally identifiable information is considered through the lens of eye-tracking data, one of the most straightforward ways of getting it is through iris textures. Iris textures are essentially like visual fingerprints, which is why it is possible to carry out authentication tasks accurately (Kumar and Passi, 2010) and this is one of the main reasons most companies do not share raw eye images and videos due to privacy reasons.[4] Even if the raw data is not shared, several researchers pointed out the inference possibilities with eye-tracking data (Liebling and Preibusch, 2014; Kröger and others, 2020), including user attributes such as age, gender, race, body mass index, sexual preference, or health status and these inferences could potentially be carried out in virtual spaces and the Metaverse as well (Bozkir and others, 2023). However, the main difference between personal attribute identification through raw data and eye movements is that with the raw data, such as iris textures, the identification is independent of the stimulus information users encounter since the processing is done at the raw eye image and video level. Therefore, the difference between the eye image and its algorithmic representation regarding which legal regime might apply remains unclear.

Furthermore, personal attribute identification, such as the inference of health status or body mass index, depends on the stimulus information that is viewed as people with different attributes explore visual stimuli in different ways, which is reflected in their gazing behaviors. For instance, there is a very low likelihood that eye-tracking data from a driving task in VR reveals the sexual preferences of the users (Bozkir and others, 2023; Rieger and Savin-Williams, 2012). Therefore, it is essential to consider the stimulus and virtual space information that users are surrounded with when considering the privacy aspects of eye-tracking data in VR/AR.

Considering the privacy risks, a few works focused on protecting the individual’s privacy when eye-tracking technologies are utilized. Differential privacy (Dwork, 2006) has been one of the approaches that was applied. It essentially uses a privacy metric to quantify the risk of an individual participating in a database, and such privacy is achieved by adding randomly generated statistical noise to the data and queries so that an adversary is never sure about whether an individual participates in a database or not. Since privacy is achieved with a significant amount of noise, it comes with the cost of decreased utility, meaning that the usefulness of the data mining-related tasks decreases. Therefore, it is essential to arrive at a trade-off where privacy is protected yet achieves good performance in data-related utility tasks.

[2] European Data Protection Board, ‘Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement’ version 2.0, 26 April 2023

[3] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, paragraph 49

[4] See, for instance, ‘Eye Tracking Privacy Notice | Meta Store’ <https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/>accessed 27 October 2023.

The eye-tracking community has shown that it is possible to achieve such a privacy-utility trade-off when eye-tracking data collected from VR/AR setups are privatized. However, researchers also indicated that finding an optimal trade-off is not trivial (Steil and others, 2019; Bozkir and others, 2021). While differential privacy approaches preserve privacy through mathematical proofs with the cost of decreased utility, more practical approaches in the same domain focused on either data downsampling or using machine learning to mitigate privacy issues, particularly to temper person re-identification tasks (David-John and others, 2021; Fuhl and others, 2021) that the adversaries can carry out. Despite these attempts, currently, no work in the domain covers both technical and legal aspects of privacy-preserving eye tracking in VR/AR.

As aforementioned, by processing eye-tracking data, it is possible to infer various information about the users and this would be the first privacy and data protection conundrum posed by eye tracking: to effectively determine whether such technologies process personal data. Further, it should be discerned whether eye-tracking data can be considered biometric and/or sensitive data and therefore merit a special degree of protection, according to EU law. Second, the lifecycle of the data processing operation should be considered: how long will the data be stored? Where? Who will have access to those data? What would happen in case of a data breach? The next part of this piece will discuss such questions by analyzing the privacy policies of several eye-tracking AR/VR devices for accessing the Metaverse and their compatibility with the GDPR.

3. Legal analysis

This piece aims to have a practical scope. Therefore, it will focus on concrete case studies to discuss the compatibility of the use of AR/VR eye-tracking devices with the GDPR. To conduct such an analysis, the English version of the privacy policies of several devices were selected. First, a distinction was made between AR and VR devices, by including multi-purpose Extended Reality (XR) devices in the scope of VR devices. Second, a further distinction was made between those devices which had an *ad hoc* privacy policy and those which forwarded the users to their general privacy policies. Analyses of devices in the first category (devices which had an *ad hoc* privacy policy) can be more granular and specific while those in the second one only allow us to consider more general aspects, as far as they apply to eye-tracking data.

To decide what eye-tracking devices for Metaverse environments should be the object of this analysis, two criteria were employed. First, for the VR devices, they were selected from the best-selling, according to market research.[5] Second, since there was no comparable data available for AR, the devices were selected following the framework of the paper ‘Speculative Privacy Concerns About AR Glasses Data Collection’ co-authored by one of the authors of this piece. Finally, the last commercial versions available were carefully chosen.

Based on the above-mentioned, the following devices were selected: Magic Leap 2, Hololens 2, Meta Quest Pro, Play Station VR2, HTC Vive PRO Eye, and Varjo XR3. Table 1 shows a summary of the selection criteria.

Table 1. AR/VR devices selected for the study

	AR	**VR**
***Ad-hoc* privacy policy**	Magic Leap 2	Meta Quest Pro
General privacy policy	Hololens 2	Play Station VR2, HTC Vive PRO Eye, Varjo XR-3

[5] Jonah Trenker, *AR & VR: market data & analysis*, Market Insights by Statista (September 2023)

a. AR devices

As eye tracking can provide various benefits such as hands-free interaction (Lystbæk and others, 2022) and human behavior understanding (Chadalavada and others, 2020), researchers aimed to integrate eye trackers in the AR devices for such or similar purposes. Especially in the earlier days of such devices, practitioners tried to come up with customized and plug-in eye-tracking solutions for AR displays such as Microsoft HoloLens (Kassner and others, 2014; Pupil Labs, 2022). While such approaches allow for low-cost and flexible solutions, the disadvantage is that obtaining unstandardized sensor data as specs of the eye-tracking sensors likely differ from one setup to another, which might make both development and compliance with privacy policies complicated as inference possibilities differ based on the sampling frequencies of the devices. More recently, several AR device vendors have integrated eye trackers into their devices by default, including Microsoft HoloLens 2 (Microsoft, 2023), Magic Leap 2 (Magic Leap, 2023), and the newly announced Apple Vision Pro (Haeney, 2023), solving the issue of unstandardized eye-tracking data collection to a great extent. In terms of data access, while HoloLens 2 and Apple Vision Pro do not provide direct access to raw eye-image data, it is possible to get this data with Magic Leap 2 with relevant permissions.

According to their privacy policy, 'Magic Leap 2 devices may collect eye tracking data including photos and videos of the eyes, pupil size and positions, gaze, vergence, center or rotation of eye, blink events, confidence of gaze and vergence, and other eye behaviors (e.g., fixation, smooth pursuit, saccades).'[6] Such data is processed 'locally, on-device' and the device 'does not collect, store, transfer or otherwise use eye tracking data in any manner'.[7] Further, third parties such as an enterprise offering Magic Leap 2's use or the app provider of an application installed on-device might have access or decided to collect and store the eye-tracking data. In such a case, the data is transferred directly without being collected, stored, transferred, or otherwise used by Magic Leap.

If we follow Article 4(14) GDPR, the abovementioned information might qualify as biometric data as long as they 'allow to confirm the unique identification of that natural person'. Therefore, AR devices' providers must ensure that no unique identification is possible from the eye-tracking data. Further, eye-tracking data could potentially fit within the sensitive data definition as data revealing racial or ethnic origin. According to Kröger and others, 'video-based eye trackers can directly record [...] skin color of a user' (Kröger and others, 2020). Skin color is covered, according to Georgieva, under the notion of racial or ethnic origin of the GDPR although Recital 51 GDPR states that 'the use of the term "racial origin" in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races' (Georgieva and others, 2020). Therefore, if they record the skin color of a user, eye-tracking devices will be processing sensitive data. Following Kröger and others, eye-tracking data can also reveal information regarding physical health, mental health, and substance use disorders (Kröger and others, 2020). Thus, if the eye-tracking data reveals health information, eye-tracking devices will be processing sensitive data according to the definition of Article 9(1) GDPR, which includes health data. Sensitive data processing is, in principle, prohibited within Europe, according to Article 9(1) GDPR. However, the regulation establishes some legal grounds to allow this processing, such as consent, as we will discuss later. Finally, regarding the access of third parties to eye-tracking data, AR devices' providers should guarantee that only the strictly necessary information is transferred (data minimization). Third parties should also comply with the mandates of the GDPR as far as the processing of eye-tracking data is concerned.

Moving on to the AR devices with no specific privacy policy, we will discuss Hololens 2. A disclaimer should, though, be made before proceeding. The resort to general privacy policies was adopted since no device-specific privacy policies were found. This does not automatically imply that such privacy policies do not (always) exist. It only implies that they are not publicly available to the knowledge of the authors of this piece. This lack of public access already raises some transparency challenges

[6] 'Magic Leap 2 Supplemental Terms and Conditions' <https://www.magicleap.com/eye-tracking> accessed 25 October 2023.

[7] ibid.

since consumers will not be able to make a properly informed purchase, at least from a privacy and data protection point of view, if access to this information is not publicly available. Further, the authors of the piece requested the abovementioned specific privacy policies with no answer, receiving the answer that there were no specific policies or with the suggestion to consult the advertisement pages of the product that provided no further clarification within this respect.

As far as Hololens 2 is concerned, the privacy-related information regarding eye-tracking cannot be found within their general privacy policy,[8] but within the developers' documentation regarding the introduction of eye-tracking within Hololens 2.[9] This might entail some problems from a privacy perspective since the (potential) consumer has to make an extra effort if they are interested in the privacy features within the Hololens 2. Instead of going to the privacy policy (the first reasonable place where one would go if they are interested in the privacy features of a product), they need to go to the developers' documentation (a place not so straightforward to be consulted by common people).

Even if they do so, the information within such a page is scarce:

> '[t]he Eye Tracking API has been designed with a user's privacy in mind; it avoids the passing of any identifiable information, particularly any biometrics. For eye-tracking capable applications, the user needs to grant the app permission to use eye-tracking information.'

First, the term passing is ambiguous from a data protection perspective (do they mean transfer? or process in any way?). Second, the sentence mentions identifiable information, particularly biometric data but omits personal information. Does this mean that they process data revealing race, for instance? Finally, regarding eye-tracking capable applications, consent needs to be given by the data subject for the information to be used. However, in case such consent is given, what data is exactly collected, processed and used and for which purposes? The sentence does not go far, leaving all these questions unsolved with the consequent uncertainty for the data subject who is still expected to consent to the use of eye-tracking information for capable applications.

b. VR devices

Eye-tracker device evolution followed a similar trend in VR as it was in AR, starting with customized solutions that could be plugged into existing VR devices in the earlier days, such as the case of HTC Vive (Kassner and others, 2014; Pupil Labs 2022). Later, different device vendors integrated their own solutions by default in their solutions such as HTC, Meta, HP, Pico, Varjo, and Fove. For instance, HTC has integrated Tobii eye trackers in the HTC Vive Pro Eye headset, which makes it possible to obtain gaze data with a frequency of up to 120 Hz and accuracies between 0.5°-1.1° (HTC Corporation, 2023). Yet due to privacy-related issues, practitioners have mainly access only to the gaze directions and size of pupils, which are detected through the Tobii software, as raw eye images and videos are indicative of personal identifiers of users via their iris textures. Like HTC, HP and Pico have also integrated Tobii eye trackers into their HP Reverb G2 Omnicept (HP Development Company, L.P., 2023), and Neo 2 Eye and Neo 3 Pro Eye headsets (Tobii, 2022a; Tobii 2022b) with frequencies up to 120Hz and 90Hz, respectively. Due to privacy reasons, raw eye images are not provided from these devices as well. Meta Quest Pro, a more recent VR device from Meta, also integrates eye trackers into their devices (Meta, 2022a). Meta states that images of the eyes are only used for estimating the gaze direction and are deleted after the processing. In addition, it is explicitly stated that these images never leave the device, meaning neither Meta nor third-party applications can access raw data that can identify users (Meta, 2022b).

[8] 'Microsoft Privacy Statement – Microsoft Privacy' <https://privacy.microsoft.com/en-us/privacystatement> accessed 4 November 2023.

[9] 'Eye Tracking Overview - Mixed Reality' (3 March 2023) <https://learn.microsoft.com/en-us/windows/mixed-reality/design/eye-tracking> accessed 4 November 2023.

Despite the attempts to preserve the privacy of individuals by limiting access to raw data, there is a certain trade-off between privacy and utility in terms of the quality of utility tasks such as gaze estimations. Since most of the state-of-the-art approaches utilize end-to-end data-driven approaches to gaze estimations or similar tasks, the use of raw eye images and videos is often a necessity. To this end, several device manufacturers followed a different path, such as Varjo and Fove. For example, Varjo VR-3 and XR-3, high-end VR and XR devices of Varjo, utilize eye trackers up to 200Hz while providing raw image and video data per each eye (Varjo, 2023a; Varjo 2023b) through their software (Varjo Developer, 2023). Similarly, Fove 0 of Fove VR also provides users with the opportunity to record raw eye image data (Fove Inc., 2023) along with other eye-related information such as pupillometry and gaze vectors. Considering the discrepancies in the specs of the VR headsets and expectations that VR space would continue growing further with the Metaverse discussions soon, privacy risks should be considered very carefully both from a technical and legal point of view.

Among the VR devices incorporating eye-tracking technology for Metaverse environments, only the Meta Quest Pro has a dedicated privacy policy. According to META's 'Eye Tracking Privacy Note',

> *'the raw image data is processed in real time on your headset and deleted once processing has been completed. We do not collect or store raw image data from the eye tracking feature on Meta servers. The abstracted gaze data is generated in real time on your headset and processed on device or Meta servers […] If you choose to calibrate eye tracking, the calibration data is stored on your device until you've chosen to delete this data in your device settings or deleted your account.'*[10]

Further, according to the same document, '[r]aw image data and calibration data are not shared with apps, even if you choose to allow access to eye tracking data.' Therefore, such data will be only processed momentarily on the device. As previously mentioned, raw image data qualifies as biometric thus sensitive data as long as it allows the unique identification of a person, and as sensitive data as long as it reveals racial or ethnic origin or concerns health. Further, the processing operation occurs irrespective of the deletion of the information or not, although this last option is much more desirable.

Moving to VR devices with a general privacy policy, we will now examine Play Station VR2, HTC Vive PRO Eye and Varjo XR3. Regarding Play Station VR2,[11] there is no mention of the processing of eye-tracking data. As previously pointed out, this makes the privacy-aware consumer's choice extremely difficult. As far as HTC Vive PRO Eye is concerned, the most relevant part of their general privacy policy is the one referring to 'Usage Data and Error Reporting'. According to this section under the heading 'Information we automatically collect',

> '[i]n addition to the information we automatically collect, [...] we may collect more detailed de-identified data about your device usage and error report data about your device [...] HTC may re-identify this data when appropriate; for example, when you request technical support, choose to use a specific HTC service or app, or create an HTC Account. [...] Usage and error data settings will not affect HTC's collection of de-identified activation data or data about specific HTC apps and services you choose to use, including HTC Account, and are otherwise subject to limitations described in this Policy.'

According to this section, HTC may re-identify the collected data when appropriate. This sentence, again, is vague. Do they mean they re-identify an individual from the collected data? Or is it the data they claim they will re-identify? Further, even if they give some examples about what is considered appropriate, they do not establish a definition that allows the reader to discern other possible re-identification scenarios. Also, since the privacy policy is deliberately vague, we cannot know if eye-tracking data are included among this potentially re-identified data or not. Further, the section continues,

[10] 'Eye Tracking Privacy Notice | Meta Store' <https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/> accessed 27 October 2023.

[11] To complete the full picture regarding the use of eye-tracking within Play Station VR2, the privacy policy of Tobii Eye Tracker 5 was also analyzed. Again, their privacy policy was general (not *ad hoc*) and contained no reference to the processing of eye-tracking data. A request for a more specific privacy policy for Tobii Eye Tracker 5 was sent, but no answer was obtained.

> ‘[o]thers, including third party analytics service providers and third party ad service providers, [...] may also automatically collect the same or similar information about you and your device when you use the Services, including personally identifiable information about your online activities over time and across third party website and applications.’

The risk of third-party access to potentially sensitive information arises again. In this case, the policy explicitly mentions that we can be dealing with personally identifiable information. However, again, we cannot truly discern if they are referring to eye-tracking data or other kinds of data.

Finally, as far as Varjo XR3 is concerned, the information about the data collected included within the general privacy policy was ‘name and contact information, other personal data necessary for maintaining the Business Partner relationship, information related to account registration, other information about subscriptions, electronic identification and behavior data’.[12] The only information that can be more or less related to the Varjo XR3 is the fact that the headset serial number will be also collected. Further, the privacy policy states that ‘[w]e do not collect or process sensitive personal data (personal data of special categories).’[13] Nevertheless, the blatant lack of information on the policy is an obstacle to any further reasoning on the topic.

c. Basis for data processing

As stated within the previous sections of the legal analysis, sensitive data processing is in principle prohibited by Article 9(1) GDPR. However, the second paragraph of such an article allows the processing in certain specific scenarios. For this piece, we will discuss the two that are most likely to apply to the processing of eye-tracking data by AR and VR devices within Metaverse environments, namely explicit consent and legitimate interest. If we consider that no sensitive and/or biometric data is processed, other bases might be also considered such as the performance of a contract (Article 6(1)(b).

I. Consent

The most used legal base that applies to the processing of eye-tracking data by VR/AR devices in Metaverse environments is consent. However, it cannot be completely discharged that other bases might apply, maybe not now but in the future such as substantial public interest (Europol Innovation Lab, 2022). According to Article 4(11) GDPR,

> ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’

Further, Articles 7 and 8 GDPR establish the conditions for consent and the conditions applicable to a child's consent concerning information society services. Privacy policies of AR/VR devices including eye tracking mainly contemplate consent as their lawful basis allowing for data processing. In general, it is an opt-in/opt-out model where the user should enable eye-tracking functionality.

However, two aspects should be discussed to make such consent completely compliant with the GDPR, namely the presence of dark patterns and information duties.

[12] ‘Privacy Policy’ (Varjo.com) <https://varjo.com/privacy-policy/> accessed 26 October 2023.

[13] ibid.

Dark patterns

According to the Spanish Data Protection Authority,

> 'The term dark patterns refers to user interfaces and user experience implementations intended to influence people's behaviour and decisions when interacting with websites, apps and social networks, so that they make decisions that are potentially detrimental to the protection of their personal data.' (Agencia Española de Protección de Datos, 2022)

If the opt-in option regarding eye tracking enabling is selected by default, excessively easy to reach and/or very difficult to reject due to the design and format of the consent form or requires no effort or minimal reading for the data subject, the conditions of Article 4(11) GDPR might not be applying in practice. The same might happen if the opt-out option is difficult to reach or burdensome for the data subject to accept. In this line, privacy policies for eye tracking by VR/AR devices should be carefully monitored in search of potential dark pattern practices.

Information duties

Whenever data processing is lawful, data controllers are expected to comply with a series of information duties towards the data subject. These duties should be carefully implemented within the privacy policies of VR/AR devices including eye tracking. Article 13 GDPR establishes the kind of information to be provided where personal data are collected from the data subject and, according to Article 12 GDPR, such information shall be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.' As previously stated, the fact that many privacy policies are general and do not include information regarding the processing of eye-tracking data contradicts such legal obligations. Let alone that, in most cases, no 'children-friendly' data protection policies exist.

II. Legitimate interest

The legitimate interest lawful base for data processing has also been argued as a possibility to allow the processing of data within Metaverse environments, for instance, within the education field. However, it is important to consider that Article 9(2) GDPR, unlike Article 6(1), does not leave margin for legitimate interest. This would leave aside the processing of biometric/sensitive eye-tracking data for legitimate interest purposes. Therefore, this base will only apply in case no sensitive and/or biometric data is processed by eye-tracking devices. This is an open question that should merit a separate study since the relevant stakeholders do not seem to be able to reach an agreement as to whether the activities performed within the Metaverse and the consequent data processing by eye-tracking devices can be considered to fit within the legitimate interest lawful base.

d. Data security and storage limitation

Finally, regarding data security requirements, Article 32 GDPR establishes obligations on both data controllers and processors. Apart from that, the principle of storage limitation from Article 5(1)(e) GDPR states that '[p]ersonal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'. In this case, the importance of the purpose of the processing should be also assessed. Privacy policies should clearly state the purposes for processing, excluding identification, comparison or other purposes that can entail the processing of sensitive/biometric data. Again, the privacy policies of AR/VR devices incorporating eye-tracking data should be carefully assessed with such principles in mind. Some policies claim that the data will be immediately deleted. However, they also claim that, in case of a crash, accessing logs might be sent to the platform providers. Further, it should be considered whether developers of AR/VR applications also have access to eye-tracking data for development purposes. Data security requirements are especially important within the case of biometric data since, in case of a data breach, unlike other data that can be replaced such as passwords or bank account numbers, they are irreplaceable. Therefore, full anonymization should be the goal to achieve. Anonymized data are not personal data and thus do not fall under the scope of application of the GDPR.

4. Policy recommendations

This paper has reviewed the main privacy and data protection issues of the use of eye tracking within VR/AR devices for Metaverse environments stemming from their privacy policies. After that, these issues have been confronted with some of the applicable GDPR provisions. From such an analysis, a series of recommendations will be proposed within the following section. Such recommendations aim to adopt more privacy-enhancing approaches and follow data protection by design and default requirements from Article 25 GDPR.

First, a new tendency towards differential privacy approaches for eye tracking has been spotted. Technical research is moving towards more privacy-aware attitudes and, consequently, a new stream of literature proposing differential privacy is currently developing (Bozkir and others, 2021; Steil and others, 2019). However, as stated in part two of this paper, the privacy-utility trade-off is one of the weak spots of differential privacy. As a reaction, the technical scholarship has proposed other solutions such as data downsampling or using machine learning. Therefore, more research should be encouraged on privacy-enhancing techniques to solve the privacy-utility conundrum without sacrificing the former. In addition to privacy-enhancing methods that add noise to preserve privacy, like differential privacy, private data representations that do not reveal user identities yet provide good performance in other tasks could be researched to preserve privacy in a similar way to cryptography, but in a computationally less expensive way, as the real-time working principle is essential for a good user experience in VR/AR.

Second, along the same line, more interdisciplinary approaches to the use of eye tracking in AR/VR devices to access Metaverse environments should be encouraged. Technical research does not happen in a societal vacuum. Privacy and data protection regulations, such as the GDPR, but also forthcoming regulations such as the EU Artificial Intelligence Act (AI Act),[14] will limit the technical capacities, reaching, in the most extreme cases, banning certain technologies or uses of such technologies.[15] Therefore, eye-tracking providers and developers should work hand in hand with regulators and policymakers to foster the development of more compliant solutions. On the other hand, legal operators should be more in contact with the industry to understand the nature of these technologies, the technological advantage they might provide, the challenges they face and the new lines of research they are working on. Inviting stakeholders will help ensure that the decisions consider the complexities of real-world uses of those technologies.

Third, access to data by third parties should be carefully monitored as to what kind of data is shared with such parties and under which legal basis. This is especially important in the case of sensitive data since, as previously stated, such data merit further protection. Additionally, within the case of biometric data, the consequence of a potential biometric data breach could be unfixable. Because of this, data protection by design and default criteria, including data security, data minimisation and storage/purpose limitation measures should be scrupulously implemented. Further, third parties in question should also ensure compliance with the GDPR and do not solely rest responsibility within the hands of the eye-tracking providers.

Fourth, since there is no clear pronouncement from the supranational Data Protection Authorities (namely, the European Data Protection Board and or European Data Protection Supervisor) regarding whether eye-tracking data and eye images used by eye-tracking headsets and glasses constitute

[14] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final

[15] See Article 5 EU AI Act.

personal data, sensitive and or biometric data, guidelines coming from them will help to ease the uncertainty for data subjects and eye-tracking providers. Considering the increasing attention that Metaverse environments and AR/VR headsets are gaining, this should be put within the priority list of Data Protection Authorities.

Fifth, privacy policies for eye-tracking within VR/AR devices to access Metaverse environments should be transparent, readable and not overwhelming. Information should be provided clearly but acknowledging at the same time the complexity of eye-tracking technology and the risks in the case of processing biometric and/or sensitive data. Special attention should be paid to children. As the gaming industry is one of the most benefitted from the opportunities posed by VR/AR and Metaverse environments, children are expected to be one of the target customers of VR/AR devices with eye-tracking functionality. Even though their parents are expected to be involved and manage the privacy and data protection requirements of the products acquired for their children, children should also be able to read and clearly understand the content of privacy policies. Regarding privacy policies, one of the main aspects that this piece has highlighted is the blatant insufficiency of general privacy policies. Such policies are extremely wide and vague, and they do not allow the data subject to make an informed decision from a consumer perspective. Along the same lines, no dark pattern practices should be allowed, and legal operators should carefully monitor privacy policies and consent forms in search of wrong practices. Otherwise, consent using eye-tracking technology would not meet the conditions imposed by the GDPR, and the legal basis for data processing would be unlawful. Accordingly, the data processing by eye-tracking devices will not follow the GDPR and, consequently, will be prohibited.

Finally, the use of the legitimate interest legal basis for data processing should be further explored by the relevant stakeholders, including scholars. Such a lawful base might allow eye-tracking data processing, for instance, within certain Metaverse environments such as for educational purposes.

5. Conclusions

This paper has discussed the use of VR/AR eye-tracking devices for Metaverse environments in light of the EU GDPR. First, it has analyzed the main privacy and data protection implications that the use of eye-tracking technologies entails from both a technical and legal perspective. Second, it has dug deeper into the nature of such technologies and the technological advantage entailed by VR/AR devices with the addition of eye tracking. After that, the privacy policies of six AR/VR devices have been discussed. Such privacy policies were *ad-hoc* for eye-tracking devices in some cases and general in the vast majority. Consequently, there is a lack of transparency on some privacy policies concerning the kind of data that is being collected and processed. In general, it can be argued that eye-tracking data can qualify as sensitive data if they reveal information about ethnic origin, are biometric data to uniquely identify a natural person or data concerning health. If that is the case, their processing is in principle prohibited unless one of the legal bases from Article 9(2) GDPR applies. Such bases could mainly be, consent on the one hand, and legitimate interest and performance of a contract for non-sensitive data on the other. For consent to apply, specific attention should be put to dark patterns and information duties and privacy policies in general. Finally, the paper proposes six policy recommendations including the need for more interdisciplinary research on privacy-enhancing techniques to solve the privacy-utility conundrum; careful monitoring of access to data by third parties, including data security and minimisation requirements; more guidance from supranational Data Protection Authorities on the processing of eye-tracking data; and more attention when designing privacy policies, especially for children.

References

Ajay Kumar and Arun Passi, "Comparison and combination of iris matchers for reliable personal authentication", Pattern Recognition (2010), 43 (3).

Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' <https://kb.osu.edu/handle/1811/72839> accessed 26 July 2023.

Alexander Plopski, Teresa Hirzle, Nahal Norouzi, Long Qian, Gerd Bruder and Tobias Langlotz, 'The Eye in Extended Reality: A Survey on Gaze Interaction and Eye Tracking in Head-worn Extended Reality', ACM Computing Surveys (2022), 55(3): 1-39.

Andrea Gallardo and others, 'Speculative Privacy Concerns About AR Glasses Data Collection' Proceedings on Privacy Enhancing Technologies.

Bernand Marr, 'The Amazing Possibilities Of Healthcare In The Metaverse' (Forbes) <https://www.forbes.com/sites/bernardmarr/2022/02/23/the-amazing-possibilities-of-healthcare-in-the-metaverse/> accessed 17 July 2023.

Bradford, Anu, The Brussels Effect: How the European Union Rules the World (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), <https://doi-org.eui.idm.oclc.org/10.1093/oso/9780190088583.001.0001>, accessed 4 Nov. 2023.

Brendan David-John, Diane Hosfelt, Kevin Butler and Eakta Jain, "A privacy-preserving approach to streaming eye-tracking data", IEEE Transactions on Visualization and Computer Graphics (2021), 27 (5).

Cynthia Dwork, "Differential Privacy", Automata, Languages and Programming (2006): 1-12.

Daniel J. Liebling and Sören Preibusch, "Privacy considerations for a pervasive eye tracking world", Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, September 2014.

'Dark Patterns: Manipulation in Internet Services' (AEPD, 19 May 2022) <https://www.aepd.es/en/prensa-y-comunicacion/blog/dark-patterns-manipulation-in-internet-services> accessed 24 July 2023.

David Haeney, 'Apple Vision Pro Apps Aren't Allowed Raw Access To The Cameras' (13 June 2023), <https://www.uploadvr.com/apple-vision-pro-apps-dont-get-access-to-the-cameras/> accessed 26 July 2023

Efe Bozkir, 'Towards Everyday Virtual Reality through Eye Tracking' <http://arxiv.org/abs/2203.15703> accessed 17 July 2023.

Efe Bozkir and others, 'Eye-Tracked Virtual Reality: A Comprehensive Survey on Methods and Privacy Challenges' (arXiv, 23 May 2023) <http://arxiv.org/abs/2305.14080> accessed 17 July 2023.

Efe Bozkir, Onur Günlü, Wolfgang Fuhl, Rafael F. Schaefer and Enkelejda Kasneci, "Differential privacy for eye tracking with temporal correlations", PLoS ONE (2021), 16 (8).

European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' version 2.0, 26 April 2023

European Data Protection Supervisor, Technology report No 1 Smart glasses and data protection, Brussels, January 2019

'Eye Tracking in Virtual Reality: A Broad Review of Applications and Challenges | SpringerLink' <https://link.springer.com/article/10.1007/s10055-022-00738-z> accessed 17 July 2023.

'Eye tracking on Hololens 2' (Microsoft, 3 March 2023) <https://learn.microsoft.com/en-us/windows/mixed-reality/design/eye-tracking> accessed 26 July 2023

'Eye tracking on Meta Quest Pro' (Meta, 2022a) <https://www.meta.com/en-gb/help/quest/articles/getting-started/getting-started-with-quest-pro/eye-tracking/> accessed 26 July 2023.

'Eye Tracking Privacy Notice | Meta Store' (Meta, 2022b) <https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/> accessed 17 July 2023.

'FOVE VR Platform Powering next generation VR & Eye Tracking applications' (Fove Inc., 2023) <https://fove-inc.com/product/fove-vr-platform/> accessed 26 July 2023

'General Privacy Policy for the Tobii Group' <https://www.tobii.com/company/privacy-policy> accessed 9 November 2023.

Gerulf Rieger, and Ritch C. Savin-Williams. "The Eyes Have It: Sex and Sexual Orientation Differences in Pupil Dilation Patterns." PLoS ONE (2012) 7(8).

'How the Metaverse Can Transform Education' (Meta, 12 April 2023) <https://about.fb.com/news/2023/04/how-the-metaverse-can-transform-education/> accessed 17 July 2023

'HP Omnicept & HP Reverb G2 Omnicept Edition' (HP Development Company, L.P., 2023) <https://www.hp.com/us-en/vr/reverb-g2-vr-headset-omnicept-edition.html> accessed 26 July 2023

'HTC Vive Pro Eye Specs' (HTC Corporation, 2023) <https://www.vive.com/sea/product/vive-pro-eye/specs/> accessed 26 July 2023

'Il Metaverso Tra Problemi Epistemologici, Etici e Giuridici - MediaLaws' <https://www.medialaws.eu/rivista/il-metaverso-tra-problemi-epistemologici-etici-e-giuridici/> accessed 17 July 2023.

Isabel Wagner, 'Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996--2021' (arXiv, 21 January 2022) <http://arxiv.org/abs/2201.08739> accessed 24 July 2023.

Isayas Berhe Adhanom, Paul MacNeilage, and Eelke Folmer. "Eye Tracking in virtual reality: A broad review of applications and challenges." Virtual Reality (2023): 1-25.

Jacob Leon Kröger, Otto Hans-Martin Lutz and Florian Müller, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' in Michael Friedewald and others (eds), Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers (Springer International Publishing 2020) <https://doi.org/10.1007/978-3-030-42504-3_15> accessed 17 July 2023.

Jia Zheng Lim, James Mountstephens and Jason Teo, 'Eye-Tracking Feature Extraction for Biometric Machine Learning' (2022) 15 Frontiers in Neurorobotics <https://www.frontiersin.org/articles/10.3389/fnbot.2021.796895> accessed 17 July 2023.

Julian Steil, Inken Hagestedt, Michael Xuelin Huang and Andreas Bulling, "Privacy-aware eye tracking using differential privacy", Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications, June 2019.

Luca Bolognini and Marco Emanuele Carpenelli, 'The Future of Personal Data in the Metaverse' (Zenodo 2022) <https://zenodo.org/record/6413046> accessed 17 July 2023.

Ludmila Georgieva and Christopher Kuner, Article 9. Processing of special categories of personal data In The EU General Data Protection Regulation (GDPR). Edited by: Christopher Kuner, Lee A. Bygrave and Christopher Docksey, Oxford University Press (2020). © Oxford University Press 2020 DOI: 10.1093/oso/9780198826491.003.0035

‘Magic Leap 2 Devices’ (Magic Leap, 23 August 2023) <https://www.magicleap.com/ml2-devices> accessed 08 November 2023.

‘Magic Leap 2 Supplemental Terms and Conditions’ <https://www.magicleap.com/eye-tracking> accessed 25 October 2023.

Marc Cortés, Analyses and insights on the potential impact of the metaverse on the education sector, Universitat Oberta de Catalunya, January 2022

Mathias N. Lystbæk, Peter Rosenberg, Ken Pfeuffer, Jens Emil Grønbæk, and Hans Gellersen, ‘Gaze-hand alignment: Combining eye gaze and mid-air pointing for interacting with menus in augmented reality’, Proceedings of the ACM Human-Computer Interaction 6, May 2022.

META, “Building Eye Tracking on Meta Quest Pro Responsibly” <https://scontent.fflr3-2.fna.fbcdn.net/v/t39.8562-6/312898144_1269308143870038_8244941952542354869_n.pdf?_nc_cat=111&ccb=1-7&_nc_sid=ae5e01&_nc_ohc=A6KaGaNQcw0AX8bb4-O&_nc_ht=scontent.fflr3-2.fna&oh=00_AfDfVOjyqaYd7yJpnQ8PoqNrD6NKi4DtJHveeHrIzeS_dA&oe=649D55F6> accessed 26 June 2023.

‘Metaverse and Privacy’ (AEPD, 29 September 2022) <https://www.aepd.es/en/prensa-y-comunicacion/blog/metaverse-and-privacy> accessed 17 July 2023.

Moritz Kassner, William Patera and Andreas Bulling, ‘Pupil: an open source platform for pervasive eye tracking and mobile gaze-based interaction’, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, September 2014.

Pedro Monteiro, Guilherme Gonçalves, Hugo Coelho, Miguel Melo and Maximino Besso, ‘Hands-free interaction in immersive virtual reality: A systematic review’, IEEE Transactions on Visualization and Computer Graphics (2021), 27(5): 2702:2713.

‘Pico Neo 2 Eye’ (Tobii, 2022a) <https://www.tobii.com/products/integration/xr-headsets/device-integrations/pico-neo-2-eye> accessed 26 July 2023

‘Pico Neo 3 Pro Eye’ (Tobii, 2022b) <https://www.tobii.com/products/integration/xr-headsets/device-integrations/pico-neo-3-pro-eye> accessed 26 July 2023

‘Policing in the Metaverse: What Law Enforcement Needs to Know’ (Europol) <https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know> accessed 17 July 2023.

‘Privacy Policy’ (Varjo.com) <https://varjo.com/privacy-policy/> accessed 26 October 2023.

Pupil Labs, ‘VR/AR, Introduction’ (01 June 2022) <https://docs.pupil-labs.com/vr-ar/> accessed 18 July 2023.

Rachel Albert, Anjul Patney, David Luebke and Joohwan Kim, ‘Latency Requirements for Foveated Rendering in Virtual Reallity’, ACM Transactions on Applied Perception (2017), 14(4): 1-13.

Ravi Teja Chadalavada, Henrik Andreasson, Maike Schindler, Rainer Palm, and Achim J. Lilienthal, ‘Bi-directional navigation intent communication using spatial augmented reality and eye-tracking glasses for improved safety in human-robot interaction’, Robotics and Computer-Integrated Manufacturing (2020), 61 (101830).

Steven Levy, 'Neal Stephenson Named the Metaverse. Now, He's Building It' Wired <https://www.wired.com/story/plaintext-neal-stephenson-named-the-metaverse-now-hes-building-it/> accessed 17 July 2023.

'Technical Specifications of Varjo VR-3' (Varjo, 2023a) <https://varjo.com/products/vr-3/> accessed 26 July 2023

'Technical Specifications of Varjo XR-3' (Varjo, 2023b) <https://varjo.com/products/xr-3/> accessed 26 July 2023

'Varjo Native SDK: Eye Tracking' (Varjo Developer, 2023) <https://developer.varjo.com/docs/native/eye-tracking> accessed 26 July 2023

'Virtual Society by Herman Narula: 9780593239971 | PenguinRandomHouse.Com: Books' (PenguinRandomhouse.com) <https://www.penguinrandomhouse.com/books/675690/virtual-society-by-herman-narula/> accessed 17 July 2023.

Wolfgang Fuhl, Efe Bozkir and Enkelejda Kasneci, "Reinforcement Learning for the Privacy Preservation and Manipulation of Eye Tracking Data", Artificial Neural Networks and Machine Learning – ICANN (2021).

Authors

Natalia Menéndez González

European University Institute

natalia.menendez@eui.eu

Efe Bozkir

University of Tübingen, Department of Computer Science

Technical University of Munich, School of Social Sciences and Technology

efe.bozkir@uni-tuebingen.de, efe.bozkir@tum.de