Data Privacy and Security Perceptions in Virtual Reality Technologies amid EU Citizens

European “Quest 2” user’s perception towards the collection and processing of personal data: An explorative qualitative study

Student Name: Pascal Vineis
Student Number: 574209

Supervisor: Mr. René König

Master Media Studies – Media & Business
Erasmus School of History, Culture and Communication
Erasmus University Rotterdam

Master’s Thesis
June 2022

Data Privacy and Security Perceptions in Virtual Reality Technologies amid EU Citizens

Abstract

In recent years the virtual reality industry oversaw important growth due to the innovative nature incorporated within Virtual Reality (VR) systems and new product launches made by high tech giants such as Meta. In fact, noticeable public figures such as Mark Zuckerberg and Bill Gates made public statements claiming that VR can revolutionize daily aspects of people's lives such as working, communicating and spending leisure time. However, given the increased public attention and use of VR technology, a substantial number of users' personal data is being generated and can potentially be used for malicious purposes. Therefore, this study aims to understand how users feel towards the collection and processing of personal data in virtual reality technology to understand public VR perception, to mitigate data privacy and security risks for safer user experience and shape the quality of future business and data regulation models.

The research question "What is the perception of European VR users towards privacy and security of personal data collection?" was answered by means of a thematic analysis to find relevant patterns amid 10 VR users utilizing the Quest 2, which is the VR headset manufactured and commercialized by Oculus, currently a sub-company of Meta. The 10 European VR users were found through Facebook and Reddit VR groups and a semi-structured interview method was used to grasp relevant responses. All interviews were transcribed to later assess the participants answers' and find 4 main themes.

In general, participants' perception on the processing of personal data collection was influenced by the reputation of the company Oculus, the sub-company of Meta. In fact, participants distrusted the company Meta being a company that retains and processes data of billions of users across the world, hence allowing the company to link identities of users across different platforms and retaining a wide range of personal data of users based on practices they conform to online. Moreover, users were skeptical towards Meta due to its history and involvement in previous controversial events of data breaching and user data exploitation. Although user' data is often collected by companies to create personalized advertisements and induce users into purchasing good, the participants responded positively and suggested personalized advertisements do not negatively affect how they use the VR system. On the other hand, the main issue presented by participants addresses the wide range of data, which is being

collected by Oculus which can be used for identification purposes for example. In fact, modern VR Head Mounted Display (HMD), upbring an unprecedent ability to identify users. Hence, the topic of "data transparency" was upbrought suggesting that transparency is an essential component for regulative authorities to comply with, to force companies such as Oculus to be transparent in how user' data is collected, used and shared. Lastly, participants expressed concerns in regard to the VR cameras incorporated in HMDs due to its intrusiveness and their capability to collect data on users' personal and private homes and spaces.

Keywords: *Virtual Reality, Data Privacy and Security, Meta, User' Data Collection, Quest 2*

Table of Contents

1. Introduction

Virtual reality (VR) technology aims to provide an innovative experience for users to immerge into a 3D computer enhanced reality which dissociates from the real world. The innovative nature of VR systems, which produces virtual sceneries through visual, haptic and auditory outputs (Roesner, 2014; Adams et al, 2018), has the potential to revolutionize daily aspects of people's lives such as working, communicating and spending leisure time (Bezegovà et al, 2018). This multi-billion-euro industry has grown rapidly in recent years due to new VR headset product launches made by high tech giants such as Meta, Samsung, Google and Vive. Furthermore, the global market value of the VR industry is expected to grow significantly in the coming years (Alsop, 2021) hence providing new challenges and concerns in regard to data privacy and security (Adams et al, 2018; Spiegel, 2018; De Guzman et al, 2019; Valluripally et al, 2020). As suggested by O'Brolcháin et al (2016) the widespread of VR technology will generate substantial number of users' personal data which can potentially be used for unethical or malicious purposes. Thus, it is important to mitigate data privacy and security risks for safer user experiences. VR systems can in fact collect data in regard to a person's physical features, technical system information and the users' environment wherein they are using the VR headset.

The aim of this study is to understand user perception of VR systems in the context of privacy and security concerns within the European Union ground laws. As of today, the literature assessing user privacy and security perception on more popular and "traditional" technologies such as tracking devices and IoTs is extensive (Hwang, 2015; Hutton et al, 2018; Lupton, 2021), however the studies addressing VR user perception on this specific topic is limited. As VR headsets have been commercially sold at large scales in the mid 2010s only, the VR system business models are relatively new meaning that little is known in regard to how users feel about data privacy and security concerns. Entwining, by means of a thematic analysis, this study will reflect upon data privacy and security concerns for the "Oculus Quest 2" headset, which is the Head Mounted Display (HMD) manufactured by "Oculus", which was purchased by Facebook (now Meta) in 2014 for 2 billion US dollars (Hoffmann et al, 2014). The following research question will be answered: "What is the perception of European VR users towards privacy and security of personal data collection?". The results of this thesis can be particularly interesting for privacy scholars, policy-makers, VR programmers, developers and marketers acting within the EU market specifically, to better understand the attitudes and behaviors of European VR users.

2. Theoretical Framework

The theoretical framework section aims to discuss the topic of data privacy and security in VR technology by critically illustrating and synthesizing relevant information and academic papers. At first, an overview of the history of VR technology is provided to understand how the technology behind it developed, and how it became a fast-growing technology which retained substantial attention from the media and consumers. Furthermore, sections containing information on the meaning of "data privacy and security" are provided, focusing on information and literature associated to the Oculus Quest 2 and privacy regulations adhering to European ground laws.

2.1 The History of Virtual Reality Technology

This section aims to provide a chronological overview of the main happenings contributing to the evolution occurring within the virtual reality industry, focusing both on technical developments of virtual technology per se, as well as the socially constructed notion of virtual reality mostly deriving from science fiction narratives.

2.1.1 Early Technological Progress and Narrative Representations in Virtual Reality

As of today, virtual reality is a well-established and advanced type of technology which is built upon centuries of ideas, visual representations, research and experiments. Already in the prehistoric era, humans drew paintings on cave walls, depicting visual representations of happenings such as hunting stories, to convey messages, ideas and facts which were later internalized and self-interpreted by tribes. Sherman & Craig (2003) suggest that cave painting was in fact one of the first mediums for self-expression and storytelling adopted by humans who later evolved and cultivated new technologies as mediums to communicate and convey messages. As the human creativity in writing, acting, drawing and creating visual representations expanded, noticeable authors and producers working in creative industries sought to immerge viewers into an imaginative and illusional world which dissociates from the real world. Yet, the culmination of the modern concept of Virtual Reality occurred due to the progress made in computer science, the creation of programming languages as well as science fiction narratives depicting data-driven virtual realities leading to an increase of awareness and public interest on the phenomenon.

In 1965, Sutherland (1965) presented the first idea of a VR space, promoting it as a computer connected display, which provides insight into a "mathematical wonderland" (p. 1)

which is not realizable in the real world. It is three years after publishing his paper "The Ultimate Display" (1965) on the notion of Virtual Reality, in 1968, that Sutherland manufactured the first ever VR headset prototype "The Sword of Domacles" with funds from the US military Advanced Research Project Agency (Dixon, 2006). The VR prototype designed by Sutherland was a head-mounted display (HMD) which incorporated a binoculus projecting a 3D computer enhanced vision with internal sensors. The vision and the screen displayed by Sutherland's prototype was emitted by cathode ray tubes (CRT) (Burdea & Coiffer, 2003) which rely on the principle of "cathodoluminescence" producing pictures as video signals, wherein electric signals are converted into light patterns (Sinclair, 2011; Dhoble et al, 2021). Sutherland's HMD graphic and field of vision was processed with a VR hardware which was primarily used to simulate a flying scene to train pilots in the US army (Burdea & Coiffer, 2003). Further advancements in HMD were made by the National Aeronautics and Space Agency (NASA) in 1981 when the Virtual Visual Environment Display (VIVED) prototype was created, with the aim of training astronauts to go into space (Burdea & Coiffer, 2003). As opposed to Sutherland's CRT HMD, NASA's VIVED was a liquid crystal display (LCD) based HMD which operates when a varying electronic voltage is applied to a layer of liquid crystal which consequently changes optical properties (Scheffer & Nehring, 1984). Today, LCD is used in modern technological mediums such as flat panel televisions and digital cameras. The VIVED prototype also incorporated a sensor tracker which could calibrate user's facial and head movements that were eventually transmitted to the computer system "PDP 11-40" (Burdea & Coiffer, 2003). The data transmitted by the sensors would eventually be transferred and processed by the computer system which could display new images corresponding to the head movements of the user.

The sense of immersion in virtual reality intensified in 1984 when Jaron Lanier, founder of "Virtual Programming Languages (VPR) Research", and Thomas Zimmerman, created the first wearable sensor gloves enabling users to be manually active within a virtual space (Faisal, 2017). After manufacturing the Data Glove, VPR was the first ever company to sell HMDs and sensor gloves in the US market leading the virtual reality industry to expand not only for military training purposes, but also for recreational purposes. The LCD based HDMs sold by VPR, namely the "eyephone 1" and the "eyephone HRX", did not receive prosperous interest in the global market as the cost of the devices were extremely high (Burdea & Coiffer, 2003). In fact, the cost of the "eyephone 1" was $10,000, the "eyephone HRX" was $49,000 and the Data Glove costed $9,000 (Borrego et al., 2015; George, 2017; Mujuru & Lopez, 2021).

In the same decade the notion of virtual reality began to retain public attention as on top of the advancements made in computer science and the establishment of companies developing VR products for recreational purposes, public writers began to write books and narratives in its regards as for the case of the science cyberpunk fiction *Neuromancer* published in 1984 by William Gibson. Gibson was amid the first authors to portray a written dystopian prediction of what the cyberspace would look alike (Csicsery-Ronay, 1992). McCaffery (1988) depicts Gibson's narrative of the cyberspace as the computer matrix, "where data dances with human consciousness, where human memory is literalized and mechanized, where multi-national information systems mutate and breed into startling new structures whose beauty and complexity are unimaginable, mystical, and (above all) non-human" (p. 218).

At the beginning of the 1990s the global commercial spectrum of virtual reality technology was enhanced by tech companies such as Nintendo, SEGA, Crystal River Engineering (CRE) contributing to production and creation of virtual reality games and new HMDs. In this period technological advancements were made by companies and computer programmers leading to an increase in computer image resolution with higher pixels meaning that significant improvements were also made in the display of images within HMDs preventing "unwanted jagged pixilation effects" (Burdea & Coiffer, 2003; p.11) which were common in previous displays. Although more improvements were made in the virtual reality technology, sales and commercial activities performed by companies weren't successful yet. For example, Nintendo's "Virtual Boy" 3D gaming console launched in 1995, which allowed gamers to immerge themselves into a dual screen display, was a failure in terms of sales and for the inability to retain public interest in the market (Zachara & Zagal, 2009). However, Boyer (2009) suggests the launch of the Nintendo "Virtual Boy" console was a revolutionary attempt, in terms of the ideological goals of the display, to adhere to utopian principles and aspirations of the modern concept and movement of virtual reality, praising the console for its cultural significance, which is still admired amid "diehard" fans and collectors of virtual reality gamers across the world (Mora-Cantallops & Bergillos, 2018).

In the previous paragraphs the linkage between virtual reality technology and science fiction narratives was mentioned as for the case of the cyberpunk fiction *Neuromancer* published by William Gibson in 1984. Yet, another science fictional story which claimed four prodigious academy awards and overall public interest right before the start of the 2000s millennium was the movie "The Matrix", directed by Lana and Lilli Wachowski (The Guardian, 2000). Mihelj et al. (2014) suggest that "The Matrix brought virtual reality out of science fiction and into the minds of the masses" (p.1). The movie depicts a dystopian world

wherein humans are unconsciously living in a virtual reality, called “The Matrix”, created by artificial intelligence machines. The idea of the movie relies on a philosophical principle involving a conflict between the “real-world” and the virtual reality wherein life is stimulated by computer-generated simulations (Gunkel, 2006). The virtual reality in “The Matrix” is represented as a “wonderland” compared to the post-apocalyptic real world, where citizens are not aware of the “truth” as they remain “ignorant of the mechanism of this deception” (Gunkel, 2006, p. 194). The same notion is limned in Plato’s “Allegory of the Cave” wherein ignorance is considered as a “bliss”, not knowing the “truth” is not harmful and remaining ignorant leads the world’s citizens to be safe and happy (Huard, 2007).

In 2001, the interactivity within virtual reality technologies outgrew with the release of the “SAS3” (also known as “SAS The Cube”) which became the first ever personal computer (PC) based cubic room gaming (Bown et al., 2017). The “SAS3” provided a different form of interactivity as gamers were immerged into a virtual reality room displaying of four screens, including the floor, equipped with projectors and sensors herded by computers which processed movements. The room of the “SAS3” was named “The Cube” to reference Plato’s “Allegory of the Cave” wherein the notions of reality and illusion are debated (Bown et al., 2017). Given the advancements in graphic development, basic PCs could be used instead of large-scaled supercomputers (Jacobson & Lewis, 2005). The virtual landscape was produced through 3D glasses which tracked head movements. Bown et al. (2017) suggest the “SAS3” was a great advancement in virtual reality technology for its graphics transmitted through basic PCs and for the “panoramic paintings” displayed increasing the sense of interactivity for users (p. 251). However, the quality of experience was limited due to a lack of tactile sensors.

3D graphic sceneries continuously advanced in the 2000s as for the example of “Street View”, the map service technology released by Google in 2007 where users could see 3D enhanced panoramic views of the real world. The service provided by Google upbrought the wider mass attention towards 3D sceneries which were still mostly perceived as “modern”. Another event which accentuated 3D popularity amid society was the release of the movie “Avatar” in 2009, directed by James Cameron. According to Yun (2010), the gargantuan success of the movie “Avatar” was a turning point for 3D technology, given the evolution of stereoscopic effects which are also used in modern VR HMDs, consequently leading people to deploy 3D technologies in their own houses such as 3D TVs.

2.1.2 Emergence of Modern VR Technology

The “re-emergence” of VR technologies occurred in 2010, when Palmer Luckey at the age of 18 years old, designed the first prototype of the Oculus Rift HMD in his parents’ garage in southern California (Greenwood, 2020). With the support of online game developers, Palmer Luckey was able to gain attention and retain funds through “Kickstarter”, a crowdfunding platform to gather funds online from the public, wherein he pledged $2.4 million (accordingly 1.7€ million with the exchange rates in 2011) to enhance the development of his Oculus Rift prototype (Kickstarter, 2016). With the help of the Kickstarter campaign, the Oculus company was officially founded in July 2012. The first prototype Oculus Rift retained widespread interest and curiosity after John Carmack, an American computer programmer, presented the HMD at the Electronic Entertainment Expo (E3) by showing a demo of the video game “Doom” (LaValle et al., 2014). The prototype was well-appreciated as it displayed a wide viewing angle, increasing the sense of immersion in the display compared to previous designed HMDs. With the aim of developing the Oculus Rift prototype, 50.000 development kits were sent to researchers, programmers and scientist around the globe, leading the prototype to be tested and used for a wide spectrum of functions such as medicine, architecture, robotics, art and military, despite the fact it was originally designed for gaming purposes (LaValle et al., 2014). In 2014, Facebook (now meta), bought Oculus for a total of $2 billion (Hoffmann et al., 2014) given Mark Zuckerberg’s interest to invest in a company that can change people’s lives (Bown et al., 2017).

In March 2016, a revolutionary event changed the VR market as the Oculus Rift became the first ever HMD of the modern era to be sold commercially (Dingman, 2021). Ever since, the market of modern VR technology HMDs expanded with other high-tech giants, such as Samsung, Google and VIVE, involved in the manufacturing and commercialization of new headsets, all of which do not need to be connected to high-graphic computers, consequently enabling users to use VR headsets into private households (Wohlgenannt et al., 2020). So far, Oculus has released five headsets, the “Rift”, “Go”, “Quest”, “Rift S” and lastly, the “Quest 2” which got released in October 2020 (Oculus, 2020). The “Quest 2” is the HMD which this paper focuses on by assessing how its users perceive its experience in relation to the privacy and security of data.

2.2 Data Privacy and Security in Virtual Reality

As this paper aims to assess the data privacy and security perceptions of virtual reality technologies amid EU member states citizens, it is relevant to clarify what “data privacy” and “data security” entail at the first place. Hence, this section will provide an overview of the difference between “privacy” and “security” contextualized within data extraction in modern technologies. Moreover, a clarification on why data privacy and security in VR technologies is relevant and imposes new concerns will be provided, focusing on the amount and variety of data which can be captured and stored.

2.2.1 Data Privacy and Security in Modern Society

Over the past two decades, technological progresses led the greater mass to become increasingly dependent on newly created technological tools radicalizing the way people live. By purposely gathering and analyzing everyday aspects of people’s life, the practice of datafication intensified (Ruckenstein & Stüll, 2017) leading Information Technology to be a paramount interest for companies and parties interested in acquiring data of people. In fact, the collection of data amid different societal segments represents a huge opportunity in government planning and business growth (Tan & Pivot, 2015). It is undeniable that digital tools, such as computers, mobiles, phones and any other kind of device connected to the internet, upbrought substantial benefits to society in a vast number of ways, enabling both private and public sectors to evolve and become increasingly efficient. Yet, as society has become increasingly dependent on such tools, a large amount of personal data is now collected, processed, and shared imposing new privacy and security threats (De Capitani et al., 2012). Although VR technology is relatively new, given that modern VR headsets started being commercialized in 2016, the market is growing exponentially and a substantial number of users’ personal data is generated, which can potentially be used for unethical or malicious purposes (O’Brolcháí et al., 2016). VR users, just as other people carrying activities online, are increasingly leaving larger “digital footprints” which can be used to acquire information about individuals consequently threatening their privacy (O’Brolcháí et al., 2016). Hence, it is important to mitigate data privacy and security risks for safer user experiences. VR systems can in fact collect data in regard to a person’s physical features, personal identity information, technical system information and the users’ environment wherein they are using the VR headset.

2.2.2 Difference between Data Privacy and Security

Although data privacy and security are often used reciprocally, a distinguishment between the two can be made as they bear different meanings and affect users differently. Jain et al. (2016) emphasize the distinguishment between the two as "data privacy is focused on the use and governance of individual data – things like setting up policies in place to ensure that consumers' personal information is being collected, shared and utilized in appropriate ways. Security concentrates more on protecting data from malicious attacks and the misuse of stolen data for profit. While security is fundamental for protecting data, it's not sufficient for addressing privacy" (p. 3).

Data privacy deals with treatment of personal and confidential data, how it is collected, processed and shared. From a business perspective, the acquirement of personal data of individuals using technological tools, such as VR headsets, can be used for a wide range of purposes, to understand consumer behavior patterns and construct predictive analytics amid which businesses can rely on to build business models. The value of data, especially "big-data", stands as a resource to improve performance, drive sales, boost operational results, with the ultimate goal of attaining profitable outcomes (McAfee et al., 2012). As businesses have developed multiple ways to capture data of citizens, new governmental regulations and policies have been introduced to regulate how business can collect, process and share information of users, to mitigate possible data privacy threats and to protect privacy rights of citizens. For example, European Union member states adhere to the article 8 of the "Charter of Fundamental Rights of the European Union" and article 16 of the "Treaty on the Functioning of the European Union", stating that every citizen has the right to the privacy and protection of personal data (European Parliament, 2016).

As businesses and institutions have consistently retained large sets of data of different population segments, the storage and security of information has become a primary interest for governmental policy makers, both for efficient governing and to mitigate possible violations and criminal activities involving the unauthorized access to such data. Currently, people are relying on cloud services to store personal data which need to be consistently supervised and monitored to prevent any breaching from happening. Acquisti (2004) in the early stages of the internet development made a distinguishment between "on-line" and "off-line" identities of people which already in the beginning of the 2000s started to become intrinsically linked and compatible. As of today, given the dependency and addiction which part of society has in the usage of modern technologies, it is popular and inevitable to have compatible "on-line" and "off-line" identities, as in the requirements to sign up for certain services and products

necessitates personal information such as name, home address, telephone number and credit card details. The compatibility between “on-line” and “off-line” identities imposes new data security risks rending the process of identification and profiling a simple process for third parties willing to retain personal information.

2.3 Data collection, usage and sharing in VR Technology

The aim of virtual reality technology is to create an illusional world wherein users can immerge themselves into and interact with surrounding features (De Paolis & Mongelli, 2015). Historically, the aim of early scientists and developers involved in programming VR HMDs and VR games, was to increase the level of immersion and interactivity within virtual spaces, by perfecting the input of data transferred to the hardware, to support responsiveness and meaningful outputs in the VR system itself. As the level of immersion and interactivity increased, today users are given a high range of flexibility and freedom within virtual spaces, hence producing a substantial amount of data which is processed and retained by the VR system itself through physical movements and tracking sensors incorporated within HMDs and the hand controllers. In fact, the type of data which can be acquired and stored in virtual reality headsets differs from other new emerged technologies such as IoTs and Augmented Reality devices, mainly due to innovative nature disposed within tracking systems. O’Brolchàin et al. (2014), well before the commercialization of modern HMDs which started in 2016, expected virtual reality technologies to become increasingly popular, yet upbringing new ethical concerns relating to the privacy and the autonomy of users. The proliferation of VR devices induces more and more users to play and make usage of the devices in personal homes, hence recording personal and private spaces through the camera internalized within HMDs such as the infrared camera incorporated in the first Oculus Rift HMD released in 2016. Adams et al. (2018) do in fact suggest that VR users can develop a sense of intrusiveness towards VR technology due to the camera sensors and the microphones incorporated. Privacy and security concerns evolving around cameras and microphones have been a point of concern in the usage of numerous devices on top of VR systems, such as smartphones and personal computers as well (Balaban, 2021).

Modern virtual reality technologies upbring an unprecedent ability to track biometric information of users’ indicative of a person’s identity, medical conditions, and mental states (Miller et al., 2020). Miller et al. (2020) conducted a study with 511 participants using Oculus headsets and hand controllers, suggesting that the system accurately identified 95% when used

for less than 5 minutes. The authors suggest that determining user's identity through biometric data can facilitate authentication and identification. The authentication and identification of users through personal biometric data can allow data processors to identify single users, access personal sensitive data, share data to third parties, generate personalized advertisings and created customized experiences (Rogers et al., 2015).

2.3.1 Evolutionary Tracking System in "Quest 2"

The "Quest 2" HMD, launched in October 2020, provides significant improvements compared to the previous Oculus' HMDs for its new designed all-in-one form factor, new sensor touch controllers, and an increase in the resolution of the vision display (Oculus, 2020). The HMD is sold at a cost of 299$ (270€), providing access to hundreds of games, live events, and innovative ways of practicing physical exercise to stay fit, all of which can be undertaken in virtual reality. The innovative nature of the "Quest 2" relies on the instant sense of immersion upon which users are accustomed, with no use of external tracking sensors or cameras amid which old VR headsets have been traditionally confined with (Meta, 2019). The technology incorporated within the "Quest 2" is able to track full range of motions as well as locating the users' headset and hand controllers. The full range provided is supported by a technology known as "six degrees of freedom" (6DoF) which addresses motion planning, spatial planning as well as automated design (Donald, 1987) which are all essential components to for designing modern VR technologies. The "Quest 2" can in fact track motions and surroundings by codifying external components to a millimetric measure, "in nearly an infinite variety of conditions found in real-world homes", to provide accurate results during the immersion in the virtual reality (Meta, 2019). To accomplish an extensive level of accuracy in computing the surroundings of users and position of the HMD along with the hand controllers, Oculus uses computer vision combined with machine algorithms that translate into an instant 3D map of users' environment. The "translation" of data is enhanced by a Simultaneous Localization and Mapping technology (SLAM) which is considered to be the "foundation" of the modern Oculus HMDs (Meta, 2019).

2.3.2 Data Collection in "Quest 2"

As of October 2020, Oculus updated its data policies providing details on what kind of information is collected when using Oculus products, as in how user information and data is collected, used and shared. A supplemental Oculus data policy overview has been released by

the company in April 2022 (Oculus, 2022) given that the “Quest 2” can now only be used by signing in trough a Facebook account. Thus, it is mandatory for users willing to play with the “Quest 2” to sign in via a Facebook account. The system enables the high-tech giant Meta to collect users’ data intrinsically across different platforms owned by the company, such as WhatsApp, Instagram and Facebook, rending it one of the most powerful companies on the world when it comes to data collection of internet users. For example, only through Facebook, Meta collects data from over 2.9 billion Facebook users across the globe (DataReportal, 2022). This paper distinguishes two types of data which are collected from Oculus: data provided by the users themselves, and data which is collected automatically without having users to fill in information.

The first type of information collected for Quest 2 users is provided by the users themselves (Oculus, 2020). Users are in fact expected to fill in mandatory information details about themselves, such as name, telephone number and email address. Further information such as the Oculus devices acquired by users can also be filled in, yet this is not a mandatory option. When purchasing a good, Meta collects information about users’ payment details such as credit card numbers and shipping details. In the Metaverse, users can navigate and explore the virtual world using an “avatar”, created and edited by the users, giving the right to Meta to retain information on the physical features of the created avatar as well the activities undertaken by the avatar in the virtual world. Further information such as interactions made both in the metaverse and with the Oculus account are subtracted, including comments, posts and messages of users. The “Oculus Privacy Policy” document (Oculus, 2020), clarifies that information about users can also derive from “others”, for example abuse reports or videos of other users. Lastly, users can provide information about their own physical features such as the estimated hand size for example.

The second type of information retained by Oculus is collected automatically. Contrarily to the data provided by users, Oculus can access user’ data provided by third-parties and partners of Oculus. Third parties include external apps, program developers and marketing partners who collaborate with Oculus and can provide information such as online purchases, achievements in game applications and demographic data. The data accessed from third parties is relatively higher for users accessing Oculus products using Facebook, given that supplemental data can be collected. For example, users accessing their accounts using Facebook are automatically linked to the data provided in other platforms owned by Meta, such as Instagram, Snapchat and WhatsApp. Furthermore, information regarding the browser history, devices and technical information connected to the Quest 2 is collected from Oculus,

meaning that the IP address, the geographical position and information regarding internet sites users interact with are collected. The most unique set of data which is collected through the Oculus Quest 2, which differs from the more traditional technologies such as phones is the so called “Environmental, Dimensions and Movement Data”, which modern HMDs rely on to enhance interactivity within virtual spaces. Environmental data represents the information related to the space and area surrounding the HMD. Dimension data, also known as “biometric data”, relates to the body composition size of different body parts. In fact, virtual reality technologies collect extensive biometric data of users which can enhance optimal immersive experiences, yet it can also create privacy risks (Dick, 2021). Although the Oculus Privacy Policy does not mention that biometric data is collected (Oculus, 2020; Oculus, 2022), Adams et al. (2018) suggest that modern HMDs represent a unique piece of commercialized technology given their capability of capturing biometric data such as facial muscle movements and eye movements.

2.3.3 Usage of user’ Data in “Quest 2”

In the Oculus Privacy Policy document provided by Oculus, an overview of how the data is used by the company is provided. Primarily, Oculus claims to collect data of users to provide a personalized experience to users, with the aim of creating customized experiences enhanced by content which is relevant and valued by users. Hence, Oculus shares content aligning and matching with the content, apps, games, online browsing history and devices of users. Ever since the beginning of the 2000s, companies have developed business models and marketing strategies to provide customized experiences to clients and potential clients, as in the case of e-commerce. In the context of online shopping for example, customized advertising benefits consumers as they are persuaded with goods and services which are relevant and well-fitting with their personal taste and browsing history. However, the enhancement of customized experiences constructed with users’ data in e-commerce and other online activities can lead to a sense of intrusiveness negatively affecting purchasing intentions (Van Doom & Hoekstra, 2013). A study conducted by Norgren & Lindqvist (2017) investigated the attitudes and perceptions of 390 Swedish VR users towards personalized virtual reality marketing. The results of the study suggested that majority of the study sample responded positively to personalized advertisements in virtual reality when being confronted with products or services aligning with previous gaming experiences. However, the study suggests that users negatively

responded to advertisements portraying content based on more sensitive information of users, such as economic preferences or relationship statuses.

On top of providing customized experience to VR users, Oculus collects user' information to develop and improve the Oculus products. By doing so, Oculus collects information regarding the feedback, input and activities persuaded by users to identify technical issues and improve services. Information regarding technical issues and problems experienced by users are valuable for companies to ameliorate the services such as hand tracking features and to manufacture new HMD' prototypes, such as the Quest 3 expected to be released in 2023.

When users access Oculus products with a Facebook account, information of users is used to "power social features". The feature enables Meta to connect users across different platforms (e.g., Instagram, Facebook, WhatsApp and Snapchat) providing benefits to users as to augment social interactivity and build personal social networks.

2.3.4 Sharing of User' data in "Quest 2"

As suggested by Bye et al. (2019), HMDs provide new ethical implications when data is shared compared to other traditional technologies mainly due to the biometric data collected amid users, such as eye-tracking data, walking behaviors, height as well as emotional and physical reactions. More personal and sensitive information in regard to users' body composition and emotional behaviors can potentially be shared by VR companies such as Oculus. The data privacy policy overview provided by Oculus, suggests that the information related to users' profile and behaviors, such as name, contact details, amount of time spent interacting with specific content, game accomplishment and the list of connections and interactions made, is shared amid third parties such as apps, developers, online content providers and business partners of Oculus. Yet, the legal privacy policy overview does not mention any specific examples of biometric data being shared with third parties for commercial and marketing purposes. User' data can be shared with service providers of Oculus, such as external companies facilitating payments transactions, providing customer service, fulfilling orders as well as companies conducting market analysis for Oculus.

The information provided by users during in-game play can also be shared by Oculus as well as other users. Information such users' Avatar, in-app profile information and in-app activity are accessible to all users. Hence, in-app activity information is commonly shared both in and out the Oculus platforms. For example, in-game video recordings and screenshots are

commonly shared on external platforms such as YouTube and Facebook to provide insights of in-game activities.

Oculus provides a statement suggesting that in the event of bankruptcy, or if it is bought by or merged with another company, users' data will be shared with other companies. The data which Meta has accumulated over the past decade, through its diverse sub-companies, namely Facebook, Oculus, Snapchat and Instagram, can be considered of great value. "When sites and apps get acquired or go bankrupt, the consumer data they have amassed may be among the companies' most valuable assets. And that has created an incentive for some online services to collect vast databases on people without giving them the power to decide which companies, or industries, may end up with their information" (Singer & Jeremy, 2015).

2.4 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the data privacy and security law imposed by the European Union (EU) in 2018, which imposes regulations, restrictions and obligations to organizations acting within the EU market and collecting data from citizens residing in the EU (European Union, 2019). The GDPR was established in order to legislatively secure the right of EU citizens to privacy, by touching upon and extending already existing laws such as the article 8 of the "Charter of Fundamental Rights of the European Union" and article 16 of the "Treaty on the Functioning of the European Union" (European Commission, 2016). The introduction of the GDPR was established due to the technological progress made over the past two decades, during which private companies such as Facebook and Google were created hence producing, retaining, collecting and sharing large amount of users' data. On top of securing privacy rights amid EU citizens, the GDPR aims to ensure liable security amid EU citizens given the outgrowing number of sensitive data being shared online, to mitigate potential threats by protecting data from malicious attacks.

The GDPR relies its laws upon seven "protection" and "accountability" principles which any institution involved in processing data of EU citizens needs to respect and adhere to. The seven principles are established in the article 5 of the GDPR. The first principle, outlines "Lawfulness, fairness and transparency" to ensure that organizations comply with the laws and regulations. To ensure lawfulness, transparency plays an important role as every stakeholder involved in the process of data processing should be aware of the main scopes of interest, ensuring that users are being informed on what data is being collected, how it is used and to who the data is shared (Wachter, 2018). The second principle outlines the "purpose limitation"

amid which companies should process data EU citizens for “specified, explicit and legitimate purposes” (European Union, 2019). As such, companies should not commence any further processing other than the explicitly mentioned interests. The third principle outlines the “minimization” of data processing clarifying that the collection of data should be minimized, and companies should only collect “necessary” data. The fourth principle emphasizes that users’ data should be accurate and be kept up to date. The fifth principle states that users’ data should not be stored for a period of time which exceeds the initial designated timeframe. The data can be stored for longer periods of time in case the data is solely used for public interest, scientific or historical purposes and comply with the article 89 of the GDPR, which provides the applicable requirements and standards for companies to comply with in order to store data for longer periods of time. The sixth principle mentions the “integrity” and “confidentiality” of data processing. “Data integrity” implies the protection of data from unauthorized changes to ensure its reliability and accuracy, whereas “confidentiality” implies that data and information of users should be protected from unauthorized viewing and access. The seventh and last principle, accounts companies committing to processing data of users responsible to demonstrate GDPR compliance, meaning they adhere to the regulations imposed by the GDPR. Companies who declare to be compliant with the GDPR, but are not able to provide evidence, are consequently recognized as “not” GDPR compliant. Institutions who fail to comply with the GDPR are subject to fines which can reach 20€ million or 4% of the firm’s global annual revenue (Hern, 2018; European Union, 2019).

As for the case of users accessing Oculus products and residing in EU member states, the GDPR gives the right to users to object to personal data processing for direct marketing and for activities involving the sharing of data with third-parties (Oculus, 2020). Article 6 of the GDPR indicates individuals making use of technological services must provide an official consent to share their personal data (Fundamental Rights Agency, 2020). Categories of data such as the “political views, religious beliefs, sexual orientation or biometric data for the purpose of uniquely identifying a natural person” need to be processed following further guidelines and conditions imposed in the Article 9 of the GDPR (Fundamental Rights Agency, 2020; p. 3). The GDPR is in fact considered the “toughest” privacy and security law existing in the whole world, providing legal protection, data privacy and security to European citizens. Given the restrictive rules imposed with the GDPR, in February 2022, Meta warned European Union regulators that it would eliminate Facebook and Instagram in EU member states (Bodoni & Deutsch, 2022). In fact, as of 2018 the EU Court of Justice partly restricted transatlantic data sharing with the United States (US), to mitigate potential privacy and security risks given the

lack of restrictions and safety measures imposed by the US government to private companies processing data of EU citizens (European Commission, 2022). The regulations imposed by the GDPR in 2018 specifically addressed businesses which offered free content online yet made money through the collection and sharing of user' data by selling targeted advertisements (Satariano, 2018). In March 2022, the US and the European Commission announced to have established a new Transatlantic Data Privacy Framework, raising unprecedent commitments from the US in increasing privacy and civil liberties protection by reforming its laws and surveillance activities (European Commission, 2022). The new agreement will facilitate the cooperation between the EU and the US, providing further economic opportunities for companies such as Meta to develop and share data of European users with US companies (European Commission, 2022)

2.5 Perceptions towards Privacy and Security

Given that modern VR headsets first started to be commercially sold in 2016 with the launch of the Oculus Rift, and later followed by the launch of supplementary HMDs made by other high-tech giants such as Sony and HTC Vive, the literature in regard to VR user' perceptions towards the privacy and security of personal data are limited, compared to other technologies such as IoTs, augmented reality systems and fitness trackers. Hence, it is important to understand how users feel in regard to the processing of personal data undertaken by powerful companies such as Meta.

2.5.1 Data Privacy and Security perceptions in the EU

In June 2020, the European Union Agency for Fundamental Rights (FRA), published the results of a survey questioning 35,000 EU residents, across all 27 EU member states, about personal opinions and experiences in regard to data privacy and protection arising from the use of technology (Fundamental Rights Agency, 2020). The results of the survey showed that in EU member states, 41% of people do not want to share personal data with private companies. Whereas the majority of the EU population (61%) agrees to share basic personal data, such as name, home address and citizenship, with public administrations such as governing bodies controlled by the state, only 37% of the population feels comfortable sharing the same basic personal data with private companies. Furthermore, the results indicate that EU member citizens are not willing to share biometric data with private companies. As such, 94% of the

population are not willing to share personal facial images and 96% are not willing to provide fingerprint scans with private companies.

The survey provided further information on the opinions of EU citizens in regard to the security of personal data. The security of data focuses on the safeguard of personal data from attacks, infringements and the stealing of data for profit (Jain et al., 2016). The cases of data breechings can have serious repercussions on individuals as well as businesses. According to the Allianz Risk Barometer (2022), a risk assessment for companies provided by Allianz SE which is one of the leading financial and healthcare service providers worldwide headquartered in Germany, cyber incidents are ranked in the top three business risks in 2022. This is due to the increase of cyber-attacks from malicious entities ever since the Covid 19 pandemic, leading private companies to accelerate the process of digitalization and individuals to become increasingly reliant on services and technological accessories to pursue everyday actions such as work and recreational activities. Given the interest of global companies such as Meta to create illusional virtual worlds, also known as the metaverse, which are increasingly retaining public attention both from firms and individuals, this technology is expected to build new channels for cyber-attacks from cybercriminals targeting businesses and individuals (Sjouwerman, 2022). Touching upon the subject of cyber security, in the EU 55% of people are concerned that cyber criminals could access their personal information without their knowledge (Fundamental Rights Agency, 2022). The survey provided by the FRA questioned public perceptions in regard to advertisers and businesses accessing personal information online without knowledge and permission, suggesting that 31% of respondents are concerned, 42% are neither/nor concerned, and 26% are not concerned at all.

An important principle associated to the processing of data from a consumer perspective is the principle of transparency. Transparency is a core principle outlined in the Article 12 of the GDPR (Fundamental Rights Agency, 2022) which states that companies and data processors have the obligation to provide information to the subjects of interest in regard to how the data is collected, used and shared. Under the GDPR, data processors need to provide information in a “concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child” (European Commission, 2018). The European Union Agency for Fundamental Rights (2020) suggests that the majority of European citizens (72%) are acknowledgeable of the privacy settings on their smartphones, however only 41% are aware of the privacy settings of all the apps downloaded. As suggested in the Oculus Privacy Policy overview (Oculus, 2020), Oculus processes data of users accessing their service with third parties including partners who own applications on

smartphone devices. Although 31% of the FRA survey are concerned when advertisers and businesses access personal information without knowledge or permission, only one in five respondents residing in the EU always read the terms and conditions provided by online services and technological tools.

The awareness that European citizens have towards the GDPR is relatively high. In fact, 69% of EU citizens have heard about the GDPR, yet no information is provided on the extent to which users are aware of their rights in the context of data privacy and security (Fundamental Rights Agency, 2022). For example, there is no statistic related to user' awareness on the right to withdraw and forbid companies to process personal data.

2.5.2 The Privacy Paradox

The "Privacy Paradox" is an important phenomenon which relates to the privacy attitudes and behaviors of citizens living in the digital age (Kokolakis, 2017). The paradox refers to the "dichotomy" between attitudes and behaviors given that users often perceive privacy as a primary concern yet act inconsistently and contrarily to what they claim (Gerber et al., 2018). In the previous section, the results of a survey conducted by the European Union Agency for Fundamental Rights (2020) were presented, showing how only 37% of European citizens claim to feel comfortable sharing personal data with private companies. However, it is uncertain whether the 63% of respondents who claim to feel uncomfortable sharing personal data with private companies, act accordingly and eventually take actions to overcome or prevent personal data from being shared. In fact, users might claim to not feel comfortable sharing personal data, yet voluntarily use digital tools which have profiling functions and use such tools to share personal life details. According to Kokolakis (2017), the privacy paradox remains a complex phenomenon to understand, yet different theories and explanations have been provided as to why so many users perceive data privacy as a primary concern and threat yet act differently.

Gerber et al. (2018) suggest that the privacy paradox phenomenon can be associated to the concept of "homo oeconomicus", translated as "economic humans". Economic humans are the type of consumers who act and make decisions accordingly to retain benefits from a certain situation (Flender & Müllet, 2012). By applying this concept to the context of privacy, users can potentially have substantial benefits by sharing personal information when using digital tools, such as increasing convenience (saving credit card data online to speed purchasing processes), acquiring financial discounts (sharing personal email to get discounts off), and

improving socialization (playing games with friends online). The concept of "homo oeconomicus", when applied to privacy contexts, can be applied to the "calculus model" (Gerber et al., 2018) which states that although the privacy risks in the digital era are many and can be severely damaging for the reputation and safety of users, if the benefits of data sharing exceed the risks, then users are often disclosing personal information and sharing personal data (Lee & Known, 2015).

The privacy calculus model however does not reflect the larger population, as it is unlikely that every user consciously thinks of the benefits and risks of sharing personal data. In certain situations, assessing the risks and benefits can be misleading as user' personal data can be collected without consumers being aware of it (Wakefield, 2013). Thus, consumers often underestimate the risks of sharing personal data simply because they do not have all necessary information to undertake a rational and "complete" decision making. Given that the information users have is "incomplete" and therefore inaccurate, the decision making of users can suffer from cognitive biases given that they furtherly adhere to certain heuristics to compensate for the incomplete information they have (Wakefield, 2013; Gerber et al., 2018). The issue is that heuristics are used by people to make judgements quickly and efficiently yet are often inaccurate. Hence, because of heuristics that certain users employ, the behavior often does not reflect the original perception and intention, hence providing an explanation behind the privacy paradox. Furthermore, Gerber et al. (2018) suggest that the majority of people employ heuristics simply because they have not suffered from privacy invasions in the past. The contrast between attitude and behavior for safeguarding personal data, is also due to the fact that users do perceive personal privacy as highly important, yet are unaware on how to protect it given the complexity and lack of experience multiple users have.

5. Methodology

This study aims to understand the data privacy and security perceptions in virtual reality technologies amid EU member citizens. Hence, this section will provide an overview of the research design and decision-making processes made in order to answer the research question "What is the perception of European VR users towards privacy and security of personal data collection?".

A qualitative research method was used as a form of inquiry to analyze and assess user' perception of data privacy and security when using VR technologies such as the Quest 2, the HMD manufactured by Oculus. A qualitative method design was utilized throughout the research in order to attain in-depth understanding and insight into user' perceptions on the

topic. As suggested by Postman (1988), insightful scientific media related studies are often driven by adopting qualitative research designs “from the power of its language, the depth of explanations, the relevance of its examples and the credibility of its theme” (p.13). The research question “What is the perception of European VR users towards privacy and security of personal data collection?” was answered by means of a thematic analysis, using semi-structured interviews to collect data from 10 VR users utilizing the Oculus Quest 2. A thematic analysis approach was used to make order of the data, segmentize and reassemble it to find relevant patterns amid the participant’s answers.

5.1 Research Sample

The research sample consisted of 10 study participants, all of whom regularly use or have regularly used the Oculus Quest 2 HMD. The aim of this research was to recruit 10 participants to later interview them and retain data relevant to understand the phenomenon of user’ perceptions on data privacy and security in virtual reality technologies. More specifically, participants were recruited to understand “why” and “how” they feel towards the privacy and security of personal data within European grounds. The 10 participants provided and fulfilled data saturation which is defined as “the point at which the data collection process no longer offers any new or relevant data” (Dworkin, 2012; p.1). Hence after interviewing 10 participants, no further participants were recruited, as the phenomenon being investigated was understood and comprehended clearly.

The 10 participants recruited for this research were found through Facebook groups and Reddit communities which refer to the Quest 2 HMD, given that this study solely focuses on participants who possess and use the Quest 2 HMD created by Oculus. Thus, several posts were shared amid groups such as “Oculus Quest 2”, “Oculus VR Society” and “Quest 2 Community” in Facebook and “r/Quest2” in Reddit, with the aim of finding Quest 2 users who’d be willing to participate in semi-structured interviews lasting approximately 45 minutes. Participants were told beforehand about the nature of the project and were provided with an informed consent document providing relevant information to ensure a safe and well-functioning interview. The study sample was chosen using a purposive sampling method. Purposive sampling is known to be a non-probability sampling wherein participants do not have qual chances of being selected (Etikan at al., 2016), yet have a specific background which can provide in-depth information about a specific phenomenon. As in the study aims to assess how European citizens perceive data privacy and security when using VR technology, the main criteria was to find participants

who regularly use VR and who live in a European Union member state, so that questions and discussions related to the GDPR could be considered valid for the study.

5.2 Data Collection

The data was collected by undertaking semi-structured interviews with the 10 recruited participants with whom the interviews were scheduled in advance and later conducted via Skype online. Individual semi-structured interviews were chosen as the method to collect data given that they are useful to "co-create meaning with interviewees by reconstructing perceptions of events and experiences" (Di Ciccio & Crabtree, 2006; p. 316). Thus, the aim of the interviews was to reconstruct perceptions of events and experiences in the context of privacy and security of personal data when using VR technology, specifically the Oculus Quest 2.

An important aspect for conducting semi-structured interviews relies upon the questioning of open-ended questions wherein the reporter has a list of predetermined questions addressing the phenomenon discussed in an openly manner. As in "openly" manner the researcher conducted the interviews in a conversational manner, by giving the chance to the participants to discuss and explore issues and topics they believed to be relevant and aligned with the main research topic and question. In fact, semi structured interviews rely upon predominant key questions which address a topic or an idea in depth, yet it is important to ensure some sort of flexibility to the respondent (Dunn, 2005; Adams, 2015). Furthermore, the interviewer maintained a friendly approach during all the interviews which can help attain quality responses as well as validity and reliability of data (Bariball & While, 1993). As suggested by Patton (2002), the validity of a information retained from interviews mainly depends on the interviewer himself. Overall, establishing a rapport between the interviewer and the respondents ensures high validity as respondents are going to feel at ease hence they are more likely to be cooperative and provide quality answers (Johnson, 2001)

The predominant questions were written prior to conducting the interviews and were constructed by following key theories and literature provided in the theoretical framework. The predominant questions were structured in three different sections. The first section of the interview questioned interviewees' general information and background in regard to the usage of the Quest 2 HMD. As shown in Appendix A, questions such as "How long have you been using VR for?", "What do you usually do with the VR?", What activities do you pursue when

using the VR?" and "Do you interact with others when you use the VR?" were asked at the beginning of the interview.

Once a general background of the respondents was attained in relation to their usage of VR, interviewees were asked questions about potential concerns and fears during VR technology usage. Furthermore, the section addressed the collection of data in the Quest 2. Thus, participants were asked what kind of data they believe is being collected and how personal data is processed. Questions addressing how participants feel towards the processing of personal data, such as biometric data and in regard to the camera and the evolutionary tracking systems incorporated within the Quest 2 were asked. Questions in this section enabled the researcher to understand how Quest 2 users feel towards the processing of data and if users were sensitive to some specific data being processed, investigating feelings of skepticism and trust. Furthermore, questions addressing data regulative systems such as the GDPR were asked. The questions included in this section were predominantly relevant to retain data that could help answer the research question, as questions relating to user' experiences and feelings in the context of personal privacy and security of data were asked.

The third section of the pre-written questions addressed how users perceive the sub-company Oculus, and the head-company Meta. For example, respondents were asked about their level of trust towards the company Meta, as well as how they feel towards Meta retaining data of billions of users across different social platforms and becoming a global data "superpower". Participants were asked if they experienced any events or heard from any news that might have influenced their perception of Oculus and Meta, hence potentially influencing their feelings towards the companies processing their personal data through the Quest 2 HMD.

The answers of the respondents were recorded after receiving their personal consent, and later transcribed using a software. Yet, all the scripts were reviewed and corrected to ensure the script fully corresponded to the exact quotes and words explicitly used by the respondents.

5.3 Data Analysis

The research question "What is the perception of European VR users towards privacy and security of personal data collection?" was answered by means of a thematic analysis, using semi-structured interviews to collect data at first and later conducting the script analysis by following Braun & Clarke's (2008) guidelines. A thematic analysis was found to be suitable for this specific research as to facilitate the classification and segmentation of the data to detect patterns, similarities and differences amongst the data set. In fact, thematic analysis is an

effective method to make sense of a large data set, by summarizing it whilst adopting a structured approach (Nowell et al., 2017).

The thematic analysis guidelines provided by Braun & Clarke (2008) rely upon six steps which have to be followed thoroughly whilst constantly maintaining a structured approach. However, the steps outlined by Braun & Clarke (2008) are not to be followed rigorously in a chronological manner, thematic analysis "is not a linear process of simply moving from one phase to the next. Instead, it is more recursive process, where movement is back and forth as needed, throughout the phases" (p. 86). For a thematic analysis to be highly effective, a constant moving back and forth between the entire script, the coded themes and the written analysis results section must be attained.

The first step conducted relied on the familiarization with the data. The familiarization of the data started right after each interview was completed and the research author reviewed the scripts to ensure all grammatic and punctuations were correct, and that all written statements and words matched with the verbal recorded statements. This stage is crucially important to ensure "accuracy" (Braun & Clarke, 2008). As suggested by Patton (2002), at the early stages of the coding no literature was reviewed to maintain an inductive approach, and to ensure that the codes detected strongly associated to the data script and not to any biases of the research author reflecting upon the previously written theoretical framework.

The second phase consisted in generating initial codes in regard to what is relevant, interesting, consistent and matching in the data set. The initial codes were detected by "breaking down" the data script. 12 initial codes relating to examples and quotes suggesting how VR users feel towards the data privacy and security whilst using VR technologies were detected in the second phase of the data analysis. Examples of initial codes included "Giving up Data to Access Services", "GDPR Loopholes", "Rejection of Data Processing", "Data Processing Unclarity", and so on.

The third phase of the analysis relies on the conjunction of the initial codes into actual themes. This step consisted in allocating each code arising from the second phase of the analysis to "overreaching" themes. Overreaching themes were themes that embodied a pattern and significance amid multiple codes. In order to facilitate the process reassembling initial codes into overreaching themes, a thematic map was designed which included main themes and sub-themes. The main themes function as "umbrellas" for the sub-themes (Vaismoradi et al., 2016).

The fourth phase consisted in reviewing the themes, by refining and constructively determining whether each theme is supported with enough codes and coherent patterns. During

this phase four themes were detected. This phase is essential to ensure the overall validity of the study, by reviewing whether each theme "accurately reflects the meaning evident in the data set as a whole" (Braun & Clarke, 2012; p. 91). The validity of each theme was enhanced by understanding and writing the essence and deeper meaning of each theme. For example, the "Meta" theme functioned as an overreaching theme combining multiple answers provided by respondents which mostly related to how Oculus users are now dependent on creating a Facebook account to access Oculus devices and services, and to how the respondents felt towards the company Meta, which mostly consisted in negative and skeptical responses. To ensure validity of each theme, the research author reviewed each quote and theme making sure their meanings were coherent and aligned with one another.

The fifth step outlined by Braun & Clarke (2012) consisted in defining and naming the themes. The process of defining each theme was already undertaken in the step number four to ensure the themes coherently aligned with the data. Braun & Clarke (2012) define this step as the process of "defining and refining", aiming to identify the "essence" of each theme. By the end of this phase, each theme was defined, and later named.

The sixth and last step consisted in producing the report. Hence, a concise and logical analysis of the themes was reported in the results section of this paper. The results and findings emerged from the thematic analysis are in fact presented and conceptualized in the results section, by relating each theme to theories and to the literature presented in the theoretical framework, and by exhibiting the relevance of the themes to answer the research question.

6. Results

This result section aims to provide a clear overview of the results arising from the thematic analysis conducted to answer the research question "What is the perception of European VR users towards privacy and security of personal data collection?". The 10 participants interviewed in this study expressed a variety of opinions in regard to the privacy and security of personal data when using VR technologies. In this results section, the four main themes are presented and interpreted in relation to the research question and the literature review. The four emerged themes are the following: *Meta, Personalized Advertising, Data Processing Response,* and *Camera Data Collection.* Out of the four emerging themes, 2 themes are constructed and presented along with sub-themes to provide further in-depth analysis and comprehension of the concepts. The theme *Meta* embodies the sub-themes *Meta Skepticism*

and *Facebook Dependency*, and the theme *Data Processing Response* embodies the themes *Data Processing Skepticism, Data Processing Acceptance* and *Data Regulation*.

6.1 Meta

During the interview participants were asked questions in regard to how they perceive the company "Meta Inc.", originally known as "Facebook Inc." before Mark Zuckerberg announced the rebrand of the company in October 2021 in a public statement: "To reflect who we are and the future we hope to build, I'm proud to share that our company is now Meta" (Meta, 2021). Oculus is in fact a sub-company of "Meta Inc." as of it was bought in 2014 for a total of $2 billion (Hoffmann et al., 2014) given Mark Zuckerberg's interest to invest in a company that can change people's lives (Brown et al., 2017).

6.1.1 Meta Skepticism

Understanding consumer's perception towards the head-company meta is essential to verify the level of trust towards Meta in the context of personal data privacy and security of users. In fact, Meta is now a major high-tech company owning multiple sub-companies and Social Network Services such as WhatsApp, Snapchat, Facebook and Instagram, leading the company to retain and process data of billions of users across the globe (Reiff, 2021). In an era wherein the wider masses have become increasingly dependent on newly created technological tools radicalizing the way people live and interact with one another, the practice of datafication intensified (Ruckenstein & Stüll, 2017) leading companies to be progressively interested in acquiring data in regard to daily aspects of people's lives. As suggested by Tan & Pivot (2015), collecting data amid different social segments represents a paramount interest for companies seeking to grow and build profits. The paramount interest for data oversaw a substantial increase in its value, leading scholars and economists to suggest that "data is the new oil" (Taffel, 2021). Yet, having companies such as Meta, retaining and processing data of billions of users across a wide spectrum of platforms and services resonated skepticisms and distrust across the study participants. The first sub-theme which emerged along with the main theme "Meta" was the "Distrust and Skepticism" for the company. For example, Participant 1, expressed skepticism and distrust towards Meta when told that the Privacy Policy Overview for Oculus products suggests collecting data of users to "offer and improve XR features" (Oculus, 2022).

Participant 1: *"That's the way they'd like (Meta) to put it. What they want. They really, they'll put a batch of people's name, names and data and things and they'll, they'll sell off to a third party to get money to get adverts to target a that's what they really mean to improve their services. What they really want is to extract more money from third parties, but yeah, that's the way they frame it."*

The distrust expressed by Participant 1 is emphasized by suggesting that Oculus allegedly does not provide a clear overview of how user' data is processed, hence taking advantage of their own customers to gain profitable outcomes.

Participant 1: *"100% of people wouldn't click yes, it will be more likely 50% less money for Facebook, which is why they're not going to be clear about it. Yeah, this is cloak and dagger nonsense and trying to lie and deceive their own customers that is disgraceful."*

Further skepticism was expressed by Participant 1 suggesting that companies like Meta exploit users and take advantage of users' inability to change and take control over personal settings.

Participant 1: *"Then the people are just giving it everything ticking terms and conditions. So, people don't realise this yet, slowly people are beginning to get some idea of it, and they think well, no, but they get the new data but haven't got a clue on how to curate their settings properly. And they just basically being shafted from all angles. Which is a shame and I think these companies are just exploiting people as simple as that."*

Participant 1: *"All they're doing is trying to make as much money as possible."*

Participant 1: *"they really try hard they make it really difficult for people to keep their privacy which is awful."*

Participant 1: *"This will be the last Oculus kit I will buy primarily because of I know how they're using it."*

A surprised feeling was pronounced by Participant 3 who was not aware that Meta, the same head-company owning Facebook, Snapchat, Instagram, and WhatsApp also owns Oculus.

> Participant 3: *"Well, now that you tell this quite concerned, because I didn't know this was all the same company. I still think that people will, like keep using it. Because people already know that what Facebook does and what Instagram does, and people still use it. But I didn't know. That's crazy."*

Furthermore, also Participants 6 and 8 expressed concerns and skepticism towards Meta being a "powerful" company which gathers substantial amount of data of billions of users across the globe, all of which are stored by one holder.

> Participant 6: *"So, I think I mean, it can it is slightly concerning that meta is such a powerful company right now that as you know, this company knows all this data about everybody and all this data, all this personal data is gathered in only one place."*

> Participant 8: *"Yeah, I think it's worrying, especially because as you said, all these apps, all these media apps are linked together in the fact that there's this massive group behind it that just can gather all that information. I think it's a bit worrying. Because as I said, I don't really know what their intentions are, but the intentions are bad. God knows what they could do from me."*

6.1.2 Facebook Dependency

The second sub-theme which emerged in relation to the data privacy and security perceptions amid European VR users relates to the manner in which Meta is now obliging users accessing Oculus services and products such as the Quest 2 to login with a Facebook account, leading users to be "Facebook dependent". In fact, after releasing the Quest 2, Facebook (now meta) "required users to login through their Facebook account, partly linking their identities to their Facebook identities that already required people to use their "real" names, which in itself was controversial" (p. 2, Saker & Frith, 2022). Given the fact that Facebook has deep access to users' lives through "specific routines and rituals" (p. 1, Debatin et al., 2009), privacy awareness and reports of privacy invasion have been culminating the company's reputation

ever since its creation in 2004 (Hodge, 2006; Debatin et al., 2009; Hull et al., 2011; Esteve, 2017). Moreover, Meta's dominance in VR can potentially raise concerns given Facebook's history "with everything from arbitrary censorship to harmful algorithms to abuses of user data to inability to deal with disinformation" (p. 2, Saker & Frith, 2022). Study participants expressed concerns on the matter, pointing out that Facebook and Oculus should not be aligned under the same "umbrella", and data should not be transferred amid the two platforms for identification purposes as suggested by Participant 2 and 5.

> Participant 2: *"they really want to have an all-in-one profile. So don't know everything about you. And it's super annoying."*

> Participant 5: *"if you use Oculus, you have to have Facebook accounts, which was also one of the main concerns, public concerns about this product."*

Concerns were raised upon the fact that all content can be lost on the Oculus account if the Facebook account is deleted or is blocked at the first place. Participant 2 explicitly pointed out the unfairness of the system wherein users can potentially lose purchased games if the Facebook profile is banned, blocked or even hacked. Participant 4 on the other hand, claims that users having concerns in regard to Facebook being connected to the Quest 2, are likely to be posting and sharing content about their personal lives.

> Participant 2: *"So your Facebook profile is connected to the profile, or you log into your headset using their Facebook profile. So, if you post something on Facebook, that's not allowed. Or some imagine being hacked and somebody does that, then your Facebook profile will be blocked or banned, then you'll also lose all your everything connected to that account. So also, the access to your stew, which you can factory reset. But then still, if you've bought any games on that account, you cannot get into it anymore, so you cannot use them. I think that's very, very wrong, because you've paid for those services*

> Participant 7: *"Yeah, I was a bit afraid of the fact that you have to have a Facebook profile in order to login in the Quest. That means that I as far as I know, I cannot for example, cancel from Facebook without losing access to the contents request."*

Participant 4: *"I think most of the time the concern comes from people that are also willingly put a lot of their personal life on this platform, which I don't. I never put I think Facebook was using probably 15 years ago at the beginning. Maybe I put some picture the time and that's it. I don't put normally personal information on social so I'm not that concerned about it."*

6.2 Personalized Advertisements

The second emerging theme pointed out and discussed during the interviews reflected the process of personalized advertising in the Quest 2. Historically, users' data in digital and online platforms have commonly been used for the purpose of creating and targeting consumers and potential consumers with personalized advertisings (Tucker, 2014). Through the practice of "data mining", which is the "field of discovering novel and potentially useful information from large amounts of data" (p.1; Baker, 2010), the creation and delivery of personalized advertisements has become a relatively easy and cheap process for companies (Teeny et al., 2021). The information collected to advertise users usually incorporates information such as demographic data, browsing history, purchase history, and personally identifying information of users, such as name, location and job (Grigorios et al., 2022). Never less, the Oculus Data Policy (Oculus, 2022) suggests that one of the purposes amid which information of users is collected, is to provide and personalize Meta products as well as providing business "services" including advertisements.

As priorly mentioned in the literature review, a study examining user' response to advertisements in virtual reality has been conducted on 390 Swedish VR users, hence suggesting that the majority of the study sample responded positively to personalized advertisements when being confronted with products or services aligning with previous gaming experiences. However, the study suggests that users negatively responded to advertisements portraying content based on more sensitive information of users, such as economic preferences or relationship statuses (Norgren & Lindqvist, 2017). Yet, in this research the study participants provided a variety of responses when asked how they feel about data processing in the Quest 2 for the scope of creating personalized advertisements directed to them.

Participant 2 suggested that Oculus mainly seeks for personal data for the purpose of creating personalized advertisements, yet also suggesting this process does not affect or manipulate them into decision making. However, Participant 2 also provided a sense of disfavor towards political advertisements during election times. Furthermore, Participant 2

suggested that user' data and advertisements can be used for "evil" purposes as for the case of the Cambridge Analytica scandal which foresaw Facebook (now Meta) being involved in a scandalous case wherein identifiable information of 87 million Facebook users were provided to the data firm Cambridge Analytica which provided analytical support to Donald Trump's and Ted Cruz's election campaigns in 2016 (Isaak & Hanna, 2018). Engliston & Carter (2021) raise concerns on the wide range of data provided to Meta, such as user' cognition, preferences and biases, all of which can be used by Meta whilst having full control over the users' closed Oculus ecosystem.

> Participant 2: *"I personally don't feel very manipulated by personalised ads, because I think that's the major thing that they do with this data. Which is also I don't mind it that much. I think I'm not so sensitive to advertisement in general, or at least I feel that way."*

> Participant 2: *"It can definitely all be used for evil, like with Cambridge Analytica scandal. I think that's really bad. I personally also don't like political adverts around the election times, because I feel that you should be able to form your own opinion in that sense."*

Participant 6 also suggested their personal insensitivity to personalized advertisements suggesting that if Oculus or any other Meta app shows personalized content which touches upon sensitive personal information, such as sexual orientation or political orientation, it is the users' responsibility to stop this from happening. In fact, Participant 6 suggests that users react differently to personalized advertisements which touch upon sensitive information.

> Participant 6: *"If, I mean, if Facebook or Instagram or any other app, or Oculus even shows you content that you think is too personalised for you or touches you know, some points of your personality that you think shouldn't be shared, like, for example, sexual orientation, or political orientation, then it's up to the user. It's up to you to the user to you know, to stop it. I think that's just up to the user because it's really hard to draw a line because it's very subjective."*

Participant 8, on the other hand suggested that personalized advertisements are immerged into people's lives daily, hence making it difficult for them to even notice ads anymore. However, Participant 8 also suggested a sense of appreciation towards targeted advertisements.

> Participant 8: *"I think that I it's a bit sad to say but I think I wouldn't even notice that much. I wouldn't even really pay attention because as I say, it's something that is already so implemented. In everyday social media. We are so used to and sometimes I think it's also good to have targeted advertisements."*

6.3 Data Processing

The third emerged theme reflects upon the opinions, feelings and judgements of the interviewed participants in relation to their personal data being processed by Oculus through the Quest 2 HMD. The manner in which Oculus devices such as the Quest 2 process data of users has been constructively covered in the literature review by assessing academic sources relating to the processing of data as well as the Oculus Data Policy found on the company's website (Oculus, 2020; Oculus 2022). The respondents' feelings towards the processing of data, as in how Oculus collects, uses and shares their personal data, enhanced different feelings amid respondents, some of whom perceived a sense of rejection and skepticism, and others who accepted the processing of personal data. Hence, two sub-themes categorizing statements and feelings of *Skepticism* and *Acceptance* have been established. A relevant notion which has been discussed and mentioned numerous times was the notion of *Data Regulation*. All participants expressed their opinions in regard to the implementation of regulative systems, such as the GDPR, to manage the processing of data and protect user' personal data in a transparent way. Hence, the third sub-theme associated to the processing of data was named *Data Transparency*.

6.3.1 Data Processing Skepticism

As suggested by the European Data Protection Supervisor (2018), which is an independent institution of the EU, active in securing privacy rights of EU citizens with respect to their personal data disposed on digital platforms, the digitization of society and the complex ecosystem of digital information has led to an intense public debate in regard to personal data being processed by companies (EDPS, 2018). Participant 1 specifically mentioned to dislike

having companies or any corporations knowing about their individual preferences for example. More specifically, Participant 1 expressed concerns on the fact that companies such as Oculus take advantage of their clients to retain personal data from with the aim of generating profits.

> Participant 1: *"I mean, I certainly you know, it's my business and I don't like any corporations knowing about what my individual preferences I mean, it's, you know, I'm not embarrassed about what affiliations or what I believe in or whatever like that, I'm quite happy to tell anybody, but I don't like his people exploiting that and making money out of me."*

Furthermore, Participant 1 suggests they deny certain accesses to Oculus as for the example of the microphone, with the scope of limiting data their own personal information processing as well as their online footprint. In fact, given the expansion and growth of Virtual Reality systems and programs, VR users are increasingly leaving larger "digital footprints" which can be used to acquire information about individuals consequently threatening their privacy (O'Brolchái et al., 2016). As priorly discussed in the theoretical framework, only 37% of EU member citizens feel comfortable sharing basic personal data, such as name, home address and citizenship, with private companies (Fundamental Rights Agency, 2022).

> Participant 1: "*I had a pretty good idea of what to expect and that's why I kind of used the clamp, turning everything off if I deny them any access to my microphone or my media*."

> Participant 1: "*You gotta be very careful to minimise your online footprint as well to keep your inherent value."*

Participant 3, 7 and 9 expressed concerns in relation to the wide range of data, which is being collected by Oculus. For example, Participant 3 expresses concerns regarding the wide range of data which can be used for user' identification purposes. In fact, modern virtual reality technologies upbring an unprecedent ability to track biometric information of users' indicative of a person's identity, medical conditions, and mental states (Miller et al., 2020). The authors suggest that determining user's identity through biometric data can facilitate authentication and identification. The authentication and identification of users through personal biometric data can allow data processors to identify single users, access personal sensitive data, share data to

third parties, generate personalized advertisings and created customized experiences (Rogers et al., 2015).

> Participant 3: *"The combination of all this data because that's why you can like with all these things, you can narrow down who the person is. And if you only have generous or older customers you have then you still don't have any personal data, really. So. I think it's the danger lies for me within the combination of all these data together."*

> Participant 9: *"I think the worrying part is that they collect a "full package" of data of users."*

> Participant 10: *"I think there should be a limit on the way that data gets gets used. If you collect something that should have a purpose and the purpose should be transparent."*

Participant 9 when asked what kind of data they believe is collected by Oculus whilst using the Quest 2 HMD, suggests data is collected in regard to eye speed and movement as well as user' fitness activity, which in a "dystopic" future could be used for malicious purposes if shared with third parties, such as health insurances, which could charge users depending on their current health state.

> Participant 7: *"So for example, my eyes my speed of movement is even tracked, so all these motion related data and they can know if I am a sporty because they do this Fitness XR things which can, you know, in a dystopic future, like Black Mirror, let's say they could even charge me for a different price in my health insurance, for example, if they find out that I'm sporty or not with this, yeah, so it's it's the perspective but yeah."*

6.3.2 Data Processing Acceptance

The previous sub-theme *Data Processing Skepticism* provided an overview of the negative and concerning statements and feelings of the study participants in relation to the processing of personal data when using the Oculus Quest 2. On the other hand, this section and sub-theme *Data Processing Acceptance* aims to provide an overview of the more compliant

responsiveness and behaviors which the study participants have towards personal data processing. Certain participants suggested it is inevitable to share some data with Oculus in order to make use of the service. Participant 8 suggests that using the Quest 2 implies a "deal" between the user and the company.

> Participant 8: *"As I said I was ready to to sacrifice maybe some privacy for in order to try this technology that I found very appealing."*

> Participant 8: *"it's almost like you make a deal. When you do these things, you you agree to to give out your information."*

Participants 1 and 2 suggest that the only way to play with the Quest 2 is to accept the terms and conditions imposed by Oculus, hence giving Oculus the right to access data of participants.

> Participant 1: *"But I mean, you have to go somewhere, sharing some sort of data otherwise you can't live so you haven't you can't buy things without sharing a certain amount of data. So, you're really going to be stuck if you don't share certain things.*"

> Participant 2: *"I check it but usually you have to accept it. So it's, it's either that or not using the application. So it depends on if I really need it. I'm not even going to read it because it could only scare me a little bit. And then I'm like, well, I need this anyway. So I would accept it."*

Participant 4, admits that collecting data amid users for identification purposes does not make "sense", hence believes user' data is collected anonymously to improve the services and products, which is one of the main justifications highlighted in the Oculus Data Policy for which Oculus collects data of users at the first place, "to power social features" and "to offer and improve XR features" (Oculus, 2022).

> Participant 4: *"I think it makes sense to collect them but it doesn't make any sense to collect them in linked to a specific person. So I think they collected probably anonymously to improve the product. Because it's very useful to have this kind of*

information if you want to improve for instance the tracking. So if you want to improve the tracking, you need probably a lot of data from the field because the treaty tracking is done with camera and condition device."

Participant 4: *"So there are a lot of different situations and I think, it makes sense to collect the data, but it doesn't really matter to know who is the owner of this data because they are not trying to sell anything."*

6.3.3 Data Transparency

The aim of this study is to understand user perception of VR systems in the context of privacy and security concerns within the European Union ground laws, hence relevant literature in relation to the legislative system imposed in the European Union has already been discussed in the theoretical framework of this paper. Yet, the topic of *Data Regulation* was a major topic of discussion with interviewees when asked about their feelings and perceptions in relation to Oculus and Meta processing their personal data when using the Quest 2. According to the Fundamental Rights Agency (2022), 69% of EU member citizens are aware of the GDPR and what it entails. Except participant 7, all partaking in the interviews for this paper were aware of what the GDPR is.

Participant 6: *"I think regulation is essential to make sure that Oculus uses this information only for their services and only for product benefit purposes or enhancing the personalised experience of the product."*

Multiple interview participants suggested that transparency is a key component of data processing, thus it should be an important component transmitted and enforced by regulative authorities. The first principle of the GDPR outlines "Lawfulness, fairness and transparency" to ensure that organizations comply with the laws and regulations. To ensure lawfulness, transparency plays an important role as every stakeholder involved in the process of data processing should be aware of the main scopes of interest, ensuring that users are being informed on what data is being collected, how it is used and to who the data is shared (Wachter, 2018). Participants 2, 6 and 8 positively address data transparency.

Participant 2: *"So I feel like as long as they keep it inside the company, then that there's nobody seeing it. So that's not a problem. They have to tell you what they do with it. So that's also nice."*

Participant 6: *"As soon as you buy the product or even before buying the product in a very transparent way is essential, so that the user is exactly aware of what of what is going on and is going to experience."*

Participant 8: *"I think transparency is the key for both Facebook itself and the user to go forward with this. Yeah, I mean, I think I think it does make me happy and more feel more safe. So yeah, it makes me feel more safe, and it makes me feel like regulations will be more and more transparent, more and more strict and good for both the user and the company."*

Participant 3 outlines the terms and conditions provided by Oculus are way too long and "unclear" as in it is challenging to understand how personal data is processed. Hence data privacy and security policies should be more transparent.

Participant 3: *"Yeah, at least I think it should be more transparent because you don't nobody reads the the terms and conditions. Because they're like their movie, their YouTube movies, which read out loud the terms and conditions would take which takes like 10 hours so nobody reads it. And you don't know where your data is going. What what contracts they have with other companies to provide them the data they collect. So I think it should be there should be a way to make it more transparent."*

6.4 Camera Data Collection

The fourth and last theme which emerged from the interview participants addressed user' concerns in relation to the camera incorporated within the HMD of Oculus. The proliferation of VR devices induces more and more users to play and make usage of the devices in personal homes, hence recording personal and private spaces through the camera internalized within HMDs such as the infrared camera incorporated in the first Oculus Rift HMD released in 2016. Adams et al. (2018) do in fact suggest that VR users can develop a sense of intrusiveness towards VR technology due to the camera sensors and the microphones

incorporated. Privacy and security concerns evolving around cameras and microphones have been a point of concern in the usage of numerous devices on top of VR systems, such as smartphones and personal computers as well (Balaban, 2021). Out of the 10 interviewed participants, 6 expressed explicit complaints and concerns in regard to the camera being incorporated in the HMD.

Participant 2 believes the cameras incorporated within the Quest 2 HMD are constantly switched on hence representing a potential threat if any entity would steal the data and have an overview of what users' personal space looks like. Furthermore, Participant 2 suggests that although they made a factory reset of their HMD, the configuration and spatial area is still saved within the headset.

> Participant 2: *"Quests 2 I think the most privacy concern thing I have a about quest 2 is that it has four cameras on the front, that are literally on all the times if anybody would steal that data, they would know what my room looks like. It could look inside my house. I think that's kind of scary. But I also hope that they have a well secured, and I say, I hope that they don't even send that anywhere. I'm pretty sure they wouldn't. I'm not sure what they would need it for. So I think it's only stored on the headset, because I've factory reset it a couple of times. And it doesn't seem to save it anywhere else than on the headset. Otherwise, I wouldn't have to do a lot of stuff again, every time I do that."*

> Participant 2: *"I think cameras are intrusive, generally knowing things about me, that's fine. I'm pretty open about my political fuse as views. And then, I'm an artist, like my deepest thoughts are out there probably somewhere. In my work, just people have to understand them. Yeah, I think I'm pretty much an open book. I don't really mind it. I just don't want people spying on me in the sense that they would know everything. But it's more like a personal sense.*

Participants 7 and 9 emphasize the fact that the Oculus Quest 2 memorize the spatial area wherein users use the device, hence representing privacy concerns.

> Participant 9: *"Oculus now has an overview on how the inside of my house is looking like. Specifically, the playing area game where I usually play with the Quest 2. For example, let's say I play in the house where I am in right now in Oria, in the space where I have my carpet and where I can't damage anything around me because I must*

move. Once I leave my house and later come back to play the device memorized the space I previously played in, meaning that it conserved and memorized the data about to my room space."

Participant 7: *"I'm totally afraid. Of course, they know everything about my house."*

Participant 4 suggests that the camera can represent a threat if for business owners who display sensitive information in front of the camera.

Participant 4: *"I can imagine if I'm a company with sensible patents and I put the device with camera in a way showing sensitive information, I would be maybe careful on this. If I ever classroom where I'm doing the training. It doesn't matter the only table and chair. It's fine, but maybe I wouldn't put it in a laboratory where I have confidential technology."*

Participant 6 suggest that the camera recording is inevitable given the fact that the sensors incorporated in the Quest 2 need to define the area of movement to ensure safety and prevent users from hitting obstacles for example. Hence, it is essential to incorporate camera in the HMD. Yet, Participant 6 would be concerned if data related to their own spatial area inside their house would be accessible to employees working in Oculus.

Participant 6: *"So I'm aware that the VR set does so so that it defines the area of movement and there's a specific area we're going to move around. So understand that it is essential that it does that also be for safety measures because maybe the if you have like some obstacles in the area where he can move, then maybe the user can get hurt or stuff. So I think it is essential that it does that."*

Participant 6: "However, it would concern me if Oculus uses information or as or just like people working employees at Oculus would have the possibility to actually look inside the house and looking look inside my house that that would concern me"

7. Conclusion

The aim of this study was to assess how VR users perceive the privacy and security of personal data when using VR technologies, specifically the Quest 2 HMD created and commercialized by Oculus, a sub-company of Meta. Hence, this final section aims to answer the research question "What is the perception of European VR users towards privacy and security of personal data collection?" by addressing theoretical implications of the literature review as well as the outcomes raised from the interviews which have been presented and discussed in the results section of the paper.

Due to the innovative nature of VR technologies which can produce virtual sceneries through visual, haptic and auditory outputs (Roesner, 2014; Adams et al, 2018), it has become a widespread idea that such innovative systems have the potential to revolutionize daily aspects of people's lives such as working, communicating and spending leisure time (Bezegovà et al, 2018). Given that the global market value of VR is significantly growing (Alsop, 2021), and VR technologies dispose of highly developed tracking sensors, new challenges and concerns are raised in regard to the privacy and security of personal data of VR users (Adams et al, 2018; Spiegel, 2018; De Guzman et al, 2019; Valluripally et al, 2020). The widespread of VR technology can in fact generate substantial number of users' personal and sensitive data which can potentially be used for unethical or malicious purposes. Thus, for the purpose of answering the research question, 10 European VR users using the Quest 2 HMD commercialized by Oculus were interviewed to investigate their feelings and perceptions towards the processing of personal data. Understanding how VR users feel towards the processing of personal data is complex, given the subjective nature and experiences amid which every VR relies on their personal opinions, perceptions and beliefs. There isn't a single opinion that conforms to entire the VR society making it challenging for VR developers, marketers and regulators to enhance and comply with certain business or regulative models that satisfy every users' freedom and ensure a high level of safety of personal data at the same time.

A thematic analysis approach was used to make order of the data, segmentize and reassemble it to find relevant patterns amid the participant's answers, all of whom covered a wide range of topics expressing similar opinions hence surging overreaching topics, relevant to understand how European VR users feel towards the privacy and security of personal data collection. A key overreaching theme was linked to the company Meta, the head-company of Oculus and other major social networking platforms such as Facebook, Snapchat and Instagram. The study participants expressed a sense of skepticism towards Meta being a

company that retains and processes data of billions of users across the world, hence allowing the company to link identities of users across different platforms and retaining a wide range of personal data of users based on practices they conform to online. The skepticism that users have mainly related to the low levels of trust towards the company, partly due to the history of Facebook being accused of developing harmful algorithms and being abusive towards users' personal data. The respondent's opinions matched with the same opinion of different scholars who suggest that privacy awareness and reports of privacy invasion have been associated to Facebook ever since its creation in 2004 (Hodge, 2006; Debatin et al., 2009; Hull et al., 2011; Esteve, 2017).

All respondents referred to personalized advertisements during the semi-structured interviews, some of whom suggested advertisements are the main reason for which Oculus collects data of VR users. Thus, online surfers, as well as VR users, are often advertised based on information such as demographic data, browsing history, purchase history, and personally identifying information of users (Grigorios et al., 2022). The Oculus Data Policy (Oculus, 2022) also suggests the main purpose of collecting user' information, is to provide personalized experiences in Meta products, including advertisements. Out of the 10 participants, only one participant expressed a sense of discomfort towards personalized advertising suggesting it is not fair for these major companies to make profit out of someone's personal information. However, all other participants suggested the collection of personal data for the purpose of creating personalized advertisements does not negatively affect personal perception and usage of VR technology.

The study participants had different responses when addressing the overall processing of personal data when using the Quest 2 HMD. Several participants expressed skeptical opinions and sentiments whereas others expressed a sense of acceptance. As suggested by O'Brolcháin et al. (2016) VR systems can increasingly leave large "digital footprints" which can be used to acquire sensitive information of users and threaten their privacy. Hence, respondents suggested they take initiations to limit the amount of data exposed in their Oculus accounts. The main issue presented by participants was related to the wide range of data, which is being collected by Oculus which can be used for identification purposes for example. In fact, modern VR HMD, upbring an unprecedent ability to identify users through biometric data for example, which is indicative of a person's identify of a person's identity, medical conditions, and mental states (Miller et al., 2020). Hence, the topic of "data transparency" was upbrought suggesting that transparency is an essential component for regulative authorities to comply

with, to force companies such as Oculus to be transparent in how user' data is collected, used and shared.

Although users were expected to provide a sense of skepticism towards the collection of biometric data, users mostly expressed concerns to data being collected through the camera of the HMD. 6 Interviewees out of 10 expressed explicit complaints and concerns in regard to the camera and the sense of intrusiveness it gives to users.

On the other hand, some respondents accepted and tolerated the collection of personal data. As such, users suggested that the only way to play with the Quest 2 is to accept the conditions imposed by Oculus, hence giving the right to Oculus to access data of participants. Using the Quest 2 was in fact described as making a "deal" with Oculus, wherein users entertain themselves with the HMD in exchange for some personal data. Other participants completely disbelieved the fact that personal data is used for identification purposes, suggesting it is only collected anonymously to improve services and products offered by Oculus.

7.1 Limitations of the study

This section addresses the limitations of the study. Some limitations can be linked to the study sample as in only 10 participants were interviewed hence providing challenges as to how reliable the study is. In fact, the study aims to assess how European VR users feel towards privacy and security of personal data collection within European ground laws, which adhere to the legislations imposed by the GDPR. Even though qualitative studies do not aim to generalize results to a wider population, but instead to provide "rich, contextualized understanding of human experiences" (Polit & Beck, 2010; p. 1), the external validity of the study can potentially be inferred. The European Union Agency for Fundamental Rights (2020) does in fact suggest citizens behavior changes amid each country in the EU, for example, Cypriote citizens are 55% more likely to share facial image data with public authorities and private companies compared to Romanian citizens. Given the qualitative nature of this study, it is unfeasible to assess whether VR user' perceptions towards privacy and security of data collection differs due to cultural dimensions for instance. Hence, a bigger and more diverse sample size could have been selected to represent the European member states.

Another limitation relies on the fact that privacy-sensitive participants may not have joined the study hence dropping out to avoid conducting an interview via skype, hence showing their own face and how they look. Hence, participants should have been told before that enabling their own camera on zoom was not required and mandatory.

7.2 Area for Future Study

This research has shown that understanding how VR users feel towards the processing of personal data is a complex task. As shown in this research, users' perceptions towards privacy and security of personal data collection are highly subjective and there is no single opinion that conforms to the whole VR society. Hence, it can be quite challenging for VR developers, marketers and regulators to comply with a universal model or regulation which guarantees safety of users yet provides companies and users enough freedom to be entertained and make use of the wide range of activities which can be undertaken through VR HMDs. Hypothetically, it would be quite impossible if all VR users perceive privacy and security of personal data collection in the same way. Yet, it could be possible that users using HMDs from different companies have different perceptions in regard to privacy and security of personal data. Hence, providing a comparative analysis assessing whether users have different opinions based on which company is processing their data, whether is Oculus, Sony, Google or Microsoft, could be relatively important to understand user behavior and if VR companies are indicators on how users perceive the privacy and security of personal data.

References

Acquisti, A. (2004). Privacy and security of personal information. In *Economics of Information Security* (pp. 179-186). Springer, Boston, MA. https://doi.org/10.1007/1-4020-8090-5_14

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics emerging: the story of privacy and security perceptions in virtual reality.In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 427-442). https://doi.org/10.13016/M2B853K5P

Adams, W. C. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation*, *4*, 492-505.

Allianz. (2022, January 18). *Allianz Risk Barometer 2022: AGCS.* AGCS Global. Retrieved April 18, 2022, from https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html#:~:text=Allianz%20Risk%20Barometer%202022%3A%20Cyber,as%20top%20global%20business%20risk&text=11th%20Allianz%20survey%3A%20Cyber%2C%20business,business%20risks%20globally%20in%202022.

Barriball, K. L., & While, A. (1993). Collecting data using a semi-structured interview: a discussion paper. *Journal of advanced nursing*, *18*(10), 328-335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Behr, K. M., Nosper, A., Klimmt, C., & Hartmann, T. (2005). Some practical considerations of ethical issues in VR research. *Presence*, *14*(6), 668-676. DOI: 10.1162/105474605775196535

Bodoni, S., & Deutsch, J. (2022, February 8). *Meta renews warning to E.U.. it will be forced to pull Facebook.* Time. Retrieved April 15, 2022, from https://time.com/6146178/meta-facebook-eu-withdraw-data/

Borrego, A., Latorre, J., Lloréns, R., Noé, E., & Keshner, E. A. (2015, June). Low-cost, room-size, and highly immersive virtual reality system for virtual and mixed reality applications. In *2015 International Conference on Virtual Rehabilitation (ICVR)* (pp. 273-277). IEEE. doi: 10.1186/s12984-019-0552-6

Bown, J., White, E., & Boopalan, A. (2017). Looking for the ultimate display: A brief history of virtual reality. In *Boundaries of self and reality online* (pp. 239-259). Academic Press. https://doi.org/10.1016/B978-0-12-804157-4.00012-8

Boyer, S. (2009). A virtual failure: Evaluating the success of Nintendo's Virtual Boy. *The Velvet Light Trap*, (64), 23-33. DOI: 10.1353/vlt.0.0039

Burdea, G. C., & Coiffet, P. (2003). *Virtual reality technology*. John Wiley & Sons.

Bye, K., Hosfelt, D., Chase, S., Miesnieks, M., & Beck, T. (2019). The ethical and privacy implications of mixed reality. In *ACM SIGGRAPH 2019 Panels* (pp. 1-2). https://doi.org/10.1145/3306212.3328138

Chryssolouris, G., Mavrikios, D., Fragos, D., & Karabatsou, V. (2000). A virtual reality-based experimentation environment for the verification of human-related factors in assembly processes. *Robotics and Computer-Integrated Manufacturing*, *16*(4), 267-276. https://doi.org/10.1007/978-94-017-2256-8_39

Csicsery-Ronay Jr, I. (1992). The Sentimental Futurist: Cybernetics and Art in William Gibson's Neuromancer. *Critique: Studies in Contemporary Fiction*, *33*(3), 221-240. https://doi.org/10.1080/00111619.1992.9937885

Datareportal. (2022, February 28). *The latest facebook stats: Everything you need to know datareportal – global digital insights*. DataReportal. Retrieved April 5, 2022, from https://datareportal.com/essential-facebook-stats-:~:text=Essential Facebook stats for 2022,'active' social media platforms.

De Capitani Di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2012). Data privacy: Definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *20*(06), 793-817. https://doi.org/10.1142/S0218488512400247

De Paolis, L. T., & Mongelli, A. (Eds.). (2015). *Augmented and Virtual Reality: Second International Conference, AVR 2015, Lecce, Italy, August 31-September 3, 2015, Proceedings* (Vol. 9254). Springer.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, *15*(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dhoble, S. J., Kalyani, N. T., Vengadaesvaran, B., & Arof, A. K. (Eds.). (2021). *Energy Materials: Fundamentals to Applications*. Elsevier.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dick, E. (2021). *Balancing User Privacy and Innovation in Augmented and Virtual Reality*. Information Technology and Innovation Foundation.

Dingman, H. (2021, March 29). *Five years of VR: A look at the greatest moments from Oculus rift to quest 2*. Oculus. Retrieved March 31, 2022, from https://www.oculus.com/blog/five-years-of-vr-a-look-at-the-greatest-moments-from-oculus-rift-to-quest-2/- :~:text=We released Oculus Rift in,headset of the modern era.

Dixon, S. (2006). A history of virtual reality in performance. *International Journal of Performance Arts & Digital Media, 2*(1)

Donald, B. R. (1987). A search algorithm for motion planning with six degrees of freedom. *Artificial Intelligence*, *31*(3), 295-353. https://doi.org/10.1016/0004-3702(87)90069-5

Dunn, K. (2005) 'Interviewing', in I. Hay (ed.) Qualitative Research Methods in Human Geography (2nd edn). Melbourne: Oxford University Press, pp. 79–105

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of sexual behavior*, *41*(6), 1319-1320. https://doi.org/10.1007/s10508-012-0016-6

EDPS. (2018, March 19). *EDPS opinion on online manipulation and personal data*. European Data Protection Supervisor. Retrieved May 11, 2022, from https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

Egliston, B., & Carter, M. (2021). Examining visions of surveillance in Oculus' data and privacy policies, 2014–2020. *Media International Australia*, 1329878X211041670. https://doi.org/10.1177/1329878X211041670

Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law*, *7*(1), 36-47. https://doi.org/10.1093/idpl/ipw026

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4. doi: 10.11648/j.ajtas.20160501.11

European Commission. (2018, August 22). *Guidelines on Transparency under Regulation*. Article29 - item. Retrieved April 18, 2022, from https://ec.europa.eu/newsroom/article29/items/622227

European Commission. (2022, March 25). *EU-US data transfers*. European Commission - European Commission. Retrieved May 3, 2022, from

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

European Commission. (2022, March 25). *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*. European Commission. Retrieved April 15, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

European Parliament. (2016, April 27). *DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. EUR. Retrieved April 5, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

European Union. (2019, February 13). *What are the GDPR fines?* GDPR.eu. Retrieved April 12, 2022, from https://gdpr.eu/fines/

European Union. (2019, February 13). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. Retrieved April 11, 2022, from https://gdpr.eu/what-is-gdpr/

Faisal, A. (2017). Computer science: Visionary of virtual reality. *Nature, 551*(7680), 298-299. DOI:10.1038/551298a

Fundamental Rights Agency. (2020, June 17). *Your rights matter: Data protection and privacy*. Your rights matter: Data protection and privacy - Fundamental Rights Survey. Retrieved April 17, 2022, from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf

Flender, C., Müller, G. (2012). Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited. In: Busemeyer, J.R., Dubois, F., Lambert-Mogiliansky, A., Melucci, M. (eds) Quantum Interaction. QI 2012. Lecture Notes in Computer Science, vol 7620. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35659-9_14

George, S. H. (2017). *Immersive Visualization of Geographic Landscapes in Virtual Reality with Emphasis on Archaeological Sites with Spiritual Significance to the Tongva People*. California State University, Fullerton. doi: 10.1093/iwc/iwz011

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security, 77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Greenwood, V. E. (2020). Reimagining Post-Pandemic Schooling in the United States: Oculus Rift as Allegory.

Grigorios, L., Magrizos, S., Kostopoulos, I., Drossos, D., & Santos, D. (2022). Overt and covert customer data collection in online personalized advertising: The role of user emotions. *Journal of Business Research, 141*, 308-320. https://doi.org/10.1016/j.jbusres.2021.12.025

Gunkel, D. J. (2006). The Virtual Dialectic: Rethinking The Matrix and its Significance. *Configurations*, *14*(3), 193-215. 10.1353/con.0.0019

Hern, A. (2018, May 21). *What is GDPR and how will it affect you?* The Guardian. Retrieved April 12, 2022, from https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you

Hoffman, H. G., Meyer III, W. J., Ramirez, M., Roberts, L., Seibel, E. J., Atzori, B., Sharar, B & Patterson, D. R. (2014). Feasibility of articulated arm mounted Oculus Rift Virtual Reality goggles for adjunctive pain control during occupational therapy in pediatric burn patients. *Cyberpsychology, Behavior, and Social Networking*, *17*(6), 397-401. doi: 10.1089/cyber.2014.0058

Huard, R. L. (2007). *Plato's political philosophy: The cave*. New York: Algora.

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: privacy issues on Facebook. *Ethics and information technology*, *13*(4), 289 302. https://doi.org/10.1007/s10676-010-9224-8

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert systems with applications*, *42*(5), 2764-2771. https://doi.org/10.1016/j.eswa.2014.11.031

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56-59. doi: 10.1109/MC.2018.3191268.

Jacobson, J., & Lewis, M. (2005). Game engine virtual reality with CaveUT. *Computer*, *38*(4), 79-82. DOI: 10.1109/MC.2005.126

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, *3*(1), 1-25. https://doi.org/10.1186/s40537-016-0059-y

Johnson, J. M. (2001). In depth Interviewing . *Sage Publication, Inc*, 103–119.https://doi.org/https://dx.doi.org/10.4135/9781412973588

Kickstarter. (2016, January 30). *Oculus rift: Step into the game*. Kickstarter. Retrieved March 31, 2022, from https://www.kickstarter.com/projects/1523379957/oculus-rift-step-into-the-game

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

LaValle, S. M., Yershova, A., Katsev, M., & Antonov, M. (2014, May). Head tracking for the Oculus Rift. In *2014 IEEE international conference on robotics and automation (ICRA)* (pp. 187-194). IEEE. DOI: 10.1109/ICRA.2014.6906608

Mandal, S. (2013). Brief introduction of virtual reality & its challenges. *International Journal of Scientific & Engineering Research*, *4*(4), 304-309.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: the management revolution. *Harvard business review*, *90*(10), 60-68. DOI : 23074865

Meta. (2019, September 25). *From the lab to the living room: The story behind Facebook's Oculus Insight Technology and a new era of consumer VR*. Tech at Meta. Retrieved April 1, 2022, from https://tech.fb.com/ar-vr/2019/08/the-story-behind-oculus-insight-technology/

Meta. (2021, October 29). *Founder's letter, 2021*. Meta. Retrieved May 9, 2022, from https://about.fb.com/news/2021/10/founders-letter/

Mihelj, M., Novak, D., & Beguš, S. (2014). Virtual reality technology and applications.

Mora-Cantallops, M., & Bergillos, I. (2018). Fan preservation of 'flopped'games and systems: The case of the Virtual Boy in Spain. *Catalan Journal of Communication & Cultural Studies*, *10*(2), 213-229. https://doi.org/10.1386/cjcs.10.2.213_1

Mujuru, T., & Lopez, C. (2021, August). Creating Virtual Reality Teaching Modules for Low-Cost Headsets. In *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference* (Vol. 85376, p. V002T02A083). American Society of Mechanical Engineers. https://doi.org/10.1115/DETC2021-72084

Nancy Carter, R. N., Bryant-Lukosius, D., & Alba DiCenso, R. N. (2014, September). The use of triangulation in qualitative research. In *Oncology nursing forum* (Vol. 41, No. 5, p. 545). Oncology Nursing Society. doi: 10.1188/14.ONF.545-547

Norgren, S., & Lindqvist, F. (2017). Consumers attitudes towards Virtual Reality Marketing in Sweden: Does Personalized Virtual Reality Marketing intrude on consumers integrity? http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-33975

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods*, *16*(1), https://doi.org/10.1177/1609406917733847

Oculus. (2020, October 11). *Oculus Privacy Policy*. Oculus. Retrieved April 6, 2022, from https://www.oculus.com/legal/privacy-policy-for-oculus-account-users/

Oculus. (2020, September 16). *Introducing oculus quest 2, the next generation of all-in-one VR*. Oculus. Retrieved March 31, 2022, from https://www.oculus.com/blog/introducing-oculus-quest-2-the-next-generation-of-all-in-one-vr-gaming/

Oculus. (2022, April 11). *Supplemental Oculus Privacy Policy*. Oculus. Retrieved April 6, 2022, from https://www.oculus.com/legal/privacy-policy/

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work, 1*(3), 261-283. https://doi.org/10.1177/1473325002001003636

Postman, Neil. (1988). Social science as moral theology. In *Conscientious objections: Stirring up*

Reiff, N. (2021, November 3). *5 companies owned by Facebook (Meta)*. Investopedia. Retrieved May 9, 2022, from https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

Rogers, C. E., Witt, A. W., Solomon, A. D., & Venkatasubramanian, K. K. (2015, September). An approach for user identification for head-mounted displays. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers* (pp. 143-146). DOI: 10.1145/2802083.2808391

Satariano, A. (2018, May 25). *U.S. News Outlets Block European readers over New Privacy Rules*. The New York Times. Retrieved May 31, 2022, from https://www.nytimes.com/2018/05/25/business/media/europe-privacy-gdpr-us.html

Scheffer, T. J., & Nehring, J. (1984). A new, highly multiplexable liquid crystal display. *Applied Physics Letters*, *45*(10), 1021-1023. https://doi.org/10.1063/1.95048

Sherman, W. R., & Craig, A. B. (2003). *Understanding virtual reality : interface, application, and design* (Ser. Morgan kaufmann series in computer graphics and geometric modeling). Morgan Kaufmann.

Sinclair, I. (2011). *Electronics simplified*. Newnes.

Singer, N., & Jeremy. (2015, June 29). *When a company is put up for sale, in many cases, your personal data is, too*. The New York Times. Retrieved April 10, 2022, from https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html

Sjouwerman, S. (2022, February 16). *Council post: Metaverse as the new attack vector and other security headlines to come in 2022*. Forbes. Retrieved April 18, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/02/15/metaverse-as-the-new-attack-vector-and-other-security-headlines-to-come-in-2022/?sh=4013dfe03d00

Sutherland, I. E. (1965). "The Ultimate Display". Proceedings of IFIP 65, vol 2, pp. 506–508

Taffel, S. (2021). Data and oil: Metaphor, materiality and metabolic rifts. *New Media & Society*, doi:10.1177/14614448211017887

Tan, Q., & Pivot, F. (2015, December). Big data privacy: changing perception of privacy. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)* (pp. 860-865). IEEE. doi: 10.1109/SmartCity.2015.176.

Teeny, J. D., Siev, J. J., Briñol, P., & Petty, R. E. (2021). A review and conceptual framework for understanding personalized matching effects in persuasion. *Journal of Consumer Psychology*, *31*(2), 382-414. https://doi.org/10.1002/jcpy.1198

The Guardian. (2000, June 5). *The matrix shines at MTV Awards*. The Guardian. Retrieved March 3, 2022, from https://www.theguardian.com/film/2000/jun/05/news1

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of marketing research*, *51*(5), 546-562. https://doi.org/10.1509/jmr.10.0355

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice.* 10.5430/jnep.v6n5p100

Van Doorn, J., & Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters*, *24*(4), 339-351. DOI : 10.1007/s11002-012-9222-1

VR Society. (2020, January 2). *History of virtual reality*. Virtual Reality Society. Retrieved March 2, 2022, from https://www.vrs.org.uk/virtual-reality/history.html

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology*, *10*(2), 266-294. https://doi.org/10.1080/17579961.2018.1527479

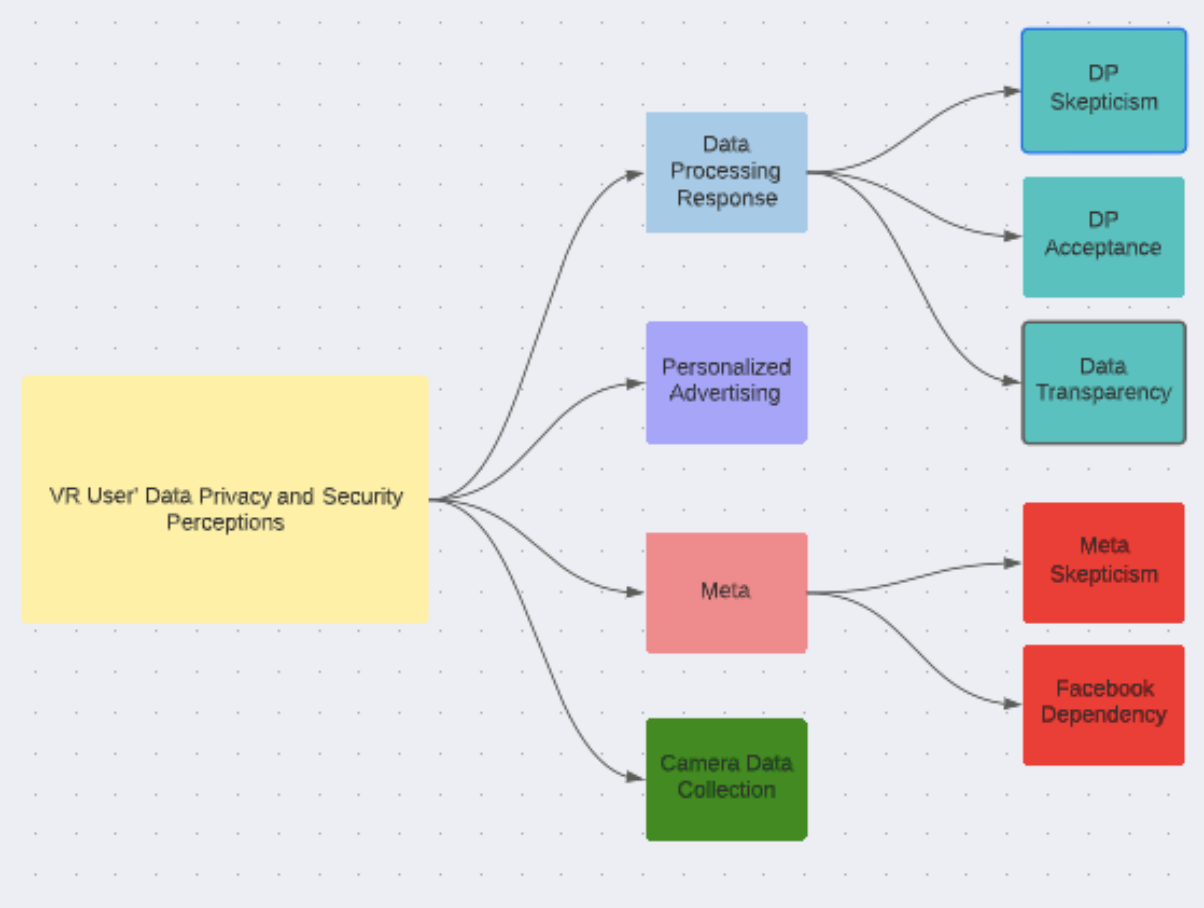
Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157-174. https://doi.org/10.1016/j.jsis.2013.01.003

Wohlgenannt, I., Simons, A., & Stieglitz, S. (2020). Virtual reality. *Business & Information Systems Engineering*, *62*(5), 455-461. https://doi.org/10.1007/s12599-020-00658-9

Yun, J. (2010). The 3D evolution after AVATAR: Welcome to 3D at homes. *Journal of Digital Research & Publishing*, 75.

Zachara, M., & Zagal, J. P. (2009, October). Challenges for success in stereo gaming: a Virtual Boy case study. In *Proceedings of the international conference on Advances in Computer Enterntainment Technology* (pp. 99-106). https://doi.org/10.1145/1690388.1690406

Appendix A


VR User' Data Privacy and Security Perceptions
Data Processing Response
Personalized Advertising
Meta
Camera Data Collection
DP Skepticism
DP Acceptance
Data Transparency
Meta Skepticism
Facebook Dependency