UNDERSTANDING THE IMPACT OF IMMERSIVE TECHNOLOGY ON THE HUMAN RIGHTS ATTITUDES WITH EMPHASIS ON PRIVACY AND DATA PROTECTION LAWS

Dissertation submitted to National Law University and Judicial Academy, Assam

in partial fulfilment for award of the degree of

MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME

Submitted by

Himangshu Sonowal

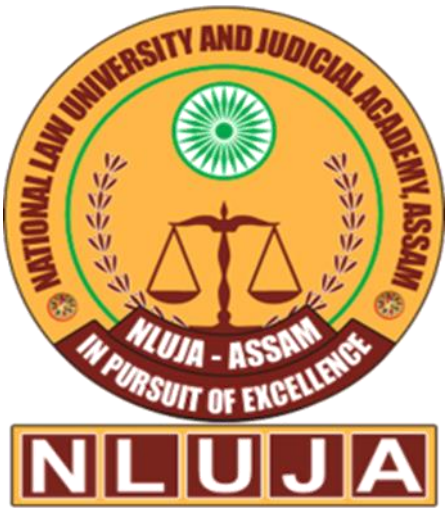
SM0222010

LLM (Semester II)

Supervised by

Dr. Gitanjali Ghosh

Assistant Professor of Law



National Law University and Judicial Academy Assam

June 2023

CONTENT

SUPERVISOR CERTIFICATE	**i**
DECLARATION	**ii**
ACKNOWLEDGEMENT	**iii**
TABLE OF CASES	**iv**
TABLE OF STATUTES	**v-vii**
TABLE OF ABBREVIATIONS	**vii-x**
1. INTRODUCTION	**1-18**
1.1. RESEARCH BACKGROUND	**1-9**
1.2. STATEMENT OF PROBLEM	**9-11**
1.3. DETAILED LITERATURE REVIEW	**11-15**
1.4. AIMS	**15**
1.5. OBJECTIVES	**15-16**
1.6. SCOPE AND LIMITATIONS	**16**
1.7. RESEARCH QUESTIONS	**16**
1.8. RESEARCH METHODS	**17**
1.9. RESEARCH DESIGN	**17-18**
2. UNDERSTANDING IMMERSIVE TECHNOLOGY	**19-70**
2.1. INTRODUCTION TO IMMERSIVE TECHNOLOGY	**19-23**
2.2. THE MECHANISM BEHIND THE FUNCTIONING OF IMMERSIVE TECHNOLOGY	**24-27**
2.2.1. VR INTERFACES	**24-26**
2.2.2. AR INTERFACES	**26-27**
2.3. SOCIAL IMPLICATIONS OF IMMERSIVE TECHNOLOGY	**28-34**
2.3.1. PSYCHOLOGICAL ATTRIBUTES ASSOCIATED WITH IMMERSIVE EXPERIENCES	**30-33**
2.3.2. CONTENT-BASED CHARACTERISTICS OF IMMERSIVE INTERFACES	**33-34**
2.4. NECESSITY OF IMPLEMENTING SAFETY MEASURES IN IMMERSIVE TECHNOLOGY	**35-43**
2.5. CHALLENGES IN IMMERSIVE TECHNOLOGY	**43-70**
2.5.1. DISCUSSION ON RISKS AND CHALLENGES DEALT WITH BY VULNERABLE USERS IN AR/VR	**44-45**

2.5.1.1. RISKS & CHALLENGES ASSOCIATED WITH PRIVACY, HEALTH, AND SAFETY FOR VULNERABLE USERS WITHIN AR/VR 45-51
2.5.1.2. RISKS AND CHALLENGES OF ACCESS AND INCLUSION FOR VULNERABLE USERS IN AR/VR 52-59
2.5.1.3. RISKS AND CHALLENGES OF BIAS & DISCRIMINATION FOR VULNERABLE USERS IN AR/VR 60-62
2.5.2. CONCEPT OF BIOMETRIC PSYCHOGRAPHY AND ITS POTENTIAL IMPLICATIONS FOR PRIVACY INFRINGEMENT 62-70
3. PRIVACY & DATA PROTECTION IN IMMERSIVE TECHNOLOGIES 71-125
3.1. RIGHT TO PRIVACY UNDER INTERNATIONAL HUMAN RIGHTS LAW 71-80
3.2. DATA PRTOECTION AND ITS PRINCIPLES 80-87
3.3. DISCUSSION ON PRIVACY & DATA PROTECTION IN AR/VR 87-125
3.3.1. INTRODUCTION 87-91
3.3.2. DISCUSSION ON COLLECTION OF USERS INFROMATION IN AR/VR 91-108
3.3.2.1. OBSERVABLE DATA 92-96
3.3.2.2. OBSERVED DATA 96-102
3.3.2.3. COMPUTED DATA 102-105
3.3.2.4. ASSOCIATED DATA 105-108
3.3.3. PRIVACY CONSIDERATIONS SPECIFIC TO USERS IN THE CONTEXT OF AR/VR 108-115
3.3.3.1. INTRODUCTION 108-109
3.3.3.2. DISCUSSION ABOUT THE RELATIONSHIP BETWEEN BIOMETRIC DATA AND THE PERSONAL AUTONOMY OF USERS OF IMMERSIVE TECHNOLOGY 109-111
3.3.3.3. CONSTRAINTS ON EXISTING MITIGATION PRACTICES & APPROACHES 112-113

3.3.3.4. AGGRAVATED SUSCEPTIBILITY OF VULNERABLE USERS TO POTENTIAL HARM 114-115
3.3.4. THE REGULATORY FRAMEWORK GOVERNING USER PRIVACY IN THE CONTEXT OF AR/VR 115-118
3.3.4.1. INTRODUCTION 115-116
3.3.4.2. EXISTING LEGAL PROVISIONS & REGULATIONS ABOUT PRIVACY IN VIRTUAL SPACE 116-117
3.3.4.3. POLICY CHALLENGES THAT ARISE IN THE CONTEXT OF SAFEGUARDING USER PRIVACY IN THE REALM OF AR/VR 117-118
3.3.5. SUGGESTIONS AND ADVICE FOR PROTECTING PRIVACY UNDER IMMERSIVE TECHNOLOGY 118-125
3.3.5.1. CREATION OF AN IMPARTIAL INNOVATIVE REGULATORY DIGITAL SPACE IN ORDER TO ADDRESS PRIVACY CONCERNS WITHIN THE DIGITAL DOMAIN 119
3.3.5.2. ADVICE AND ELUCIDATION ON THE IMPLEMENTATION OF THE EXISTING PRIVACY LAWS IN THE VIRTUAL SPACE 119-120
3.3.5.3. RECOMMENDATION TO CONSIDER REFORMING PRIVACY LAWS WHICH IMPOSE UNNECESSARY LIMITATION ON THE USE OF AR/VR 120-121
3.3.5.4. DEVELOPING REGULATIONS TO MITIGATE POTENTIAL RISKS 121-123
3.3.5.5. IMPLEMENTATION OF NATIONAL PRIVACY LEGISLATION TO HARMONIZE COMPLIANCE REQUIREMENTS AND FACILITATE INNOVATIVE PRACTICES 123
3.3.5.6. ENDORSEMENT OF VOLUNTARY MEASURES TO SAFEGUARD USER PRIVACY IN VIRTUAL SPACE 124-125
4. IMMERSIVE TECHNOLOGY- A WAY FORWARD 126-140
4.1. INTRODUCTION 126-127
4.2. THE CURRENT LEGAL SCENARIO 127-128

4.3. IMPLICATIONS OF BIOMETRIC PSYCHOGRAPHY ON HUMAN RIGHTS **129-130**
4.4. VULNERABILITIES AND EXPERIENCES IN IMMERSIVE TECHNOLOGY **130-132**
4.5. HUMANITARIAN SOLUTION TO HUMAN RIGHTS ISSUES IN IMMERSIVE TECHNOLOGY **132-140**
4.5.1. ESTABLISHING VALUE-BASED HEURISTICS AND ENSURING THAT EXPERIENCE RULES ARE CLEARLY UNDERSTOOD BY USERS **132-134**
4.5.2. DIFFERENT LEVELS OF IDENTIFICATION WITHIN CONTENT MODERATION LAYERS IN THE VIRTUAL SPACE **135-137**
4.5.3. IMPLEMENTING A RATING-BASED SYSTEM FOR ENTERTAINMENT IN DIGITAL SPACE **137**
4.5.4. PROTECTION OF PRIVACY BY GIVING CONTROL WITHIN VIRTUAL SPACES OVER THE COLLECTION OF DATA AND STORAGE OF DATA **137-138**
4.5.5. CREATING INDUSTRY-WIDE CODES OF CONDUCT **139-140**
5. CONCLUSION AND SUGGESTIONS **141-146**
5.1. FINDINGS **141-144**
5.2. CONCLUSIONS **144-146**
5.3. SUGGESTIONS **146**
BIBLIOGRAPHY **xi-xxvi**

SUPERVISOR CERTIFICATE

This is to certify that **HIMANGSHU SONOWAL** has completed his dissertation titled **"UNDERSTANDING THE IMPACT OF IMMERSIVE TECHNOLOGY ON THE HUMAN RIGHTS ATTITUDES WITH EMPHASIS ON PRIVACY AND DATA PROTECTION LAWS"** under my supervision for the award of the degree of **MASTER OF LAWS/ ONE YEAR LL.M DEGREE PROGRAMME of National Law University and Judicial Academy, Assam.**

Date:

Dr. Gitanjali Ghosh

Assistant Professor of Law

National Law University and Judicial Academy, Assam

DECLARATION

I, **HIMANGSHU SONOWAL**, do hereby declare that the dissertation titled **"UNDERSTANDING THE IMPACT OF IMMERSIVE TECHNOLOGY ON THE HUMAN RIGHTS ATTITUDES WITH EMPHASIS ON PRIVACY AND DATA PROTECTION LAWS"** submitted by me for the award of the degree of **MASTER OF LAWS/ ONE YEAR LL.M. DEGREE PROGRAMME of National Law University and Judicial Academy, Assam** is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date:

HIMANGSHU SONOWAL

SM0222010

National Law University and Judicial Academy, Assam

ACKNOWLEDGEMENT

I would like to express my profound gratitude to my Supervisor, Dr Gitanjali Ghosh, for her unwavering and consistent assistance, as well as her scholarly guidance and advice throughout the preparation of this dissertation. Her valuable feedback and suggestions significantly influenced the development of the research idea, for which I am sincerely appreciative and indebted.

Furthermore, I would also like to express my gratitude to the Librarian, Assistant Librarian, and Library staff members of the National Law University and Judicial Academy Assam, whose assistance and support have been invaluable to me. Each of them has helped me locate and obtain the necessary academic materials for conducting research.

Finally, I would like to extend my sincere appreciation and gratitude to the entire National Law University and Judicial Academy Assam staff for their invaluable assistance and unwavering support throughout my research endeavour. Their guidance and assistance have been instrumental in facilitating my progress and ensuring that I had access to all available resources. The assistance and contributions provided by them have been of great benefit to me.

Yours Sincerely

Himangshu Sonowal

TABLE OF CASES

1. *A.K. Gopalan v. State of Madras*
2. *Facebook-Cambridge Analytica Scandal (Vincent John Green and Mark Newman v. Cambridge Analytica Ltd and Others.)*
3. *Justice K.S. Puttaswamy v. Union of India*
4. *Kharak Singh v. State of Uttar Pradesh*
5. *Maneka Gandhi v. Union of India*
6. *M.P. Sharma v. Satish Chandra, District Magistrate, Delhi*
7. *Rustom Cavasji Cooper v. Union of India*

TABLE OF STATUTES

NATIONAL LAWS

1791	First and Fourth Amendment Rights
1935	Delaware Administrative Code
1950	Constitution of India
1973	Revised Code of Washington
1974	Privacy Act (USA)
1979	Telecommunication and Interception Act of Australia
1986	The Electronic Communications Privacy Act
1988	Australian Privacy Act
1996	China Telecommunication Act
1996	The Health Information and Portability and Accountability Act (HIPAA)
1998	UK Data Protection Act
1999	The Wireless Communication and Public Safety Act
2000	Indian Information Technology Act
2000	Family Educational Rights and Privacy Act
2008	Indian Information Technology (Amendment) Act
2008	The Illinois Biometric Information Privacy Act
2009	Generally Accepted Privacy Principles (GAPP)
2016	The Delaware Online Privacy and Protection Act
2018	The California Consumer Privacy Act (CCPA)
2019	Data Protection Bill of India
2021	EU's preliminary AI Regulation
2021	UK Online Safety Bill
2021	Texas Business and Commerce Code
2023	My Health My Data Act
2024	The Texas Data Privacy and Security Act

INTERNATIONAL INSTRUMENTS

1948	United Nations Declaration of Human Rights
1948	American Declaration of the Rights and Duties of Man
1953	European Convention on Human Rights
1969	American Convention on Human Rights
1976	International Covenant on Civil and Political Rights
1981	Council of Europe Convention 108 for the Protection of Individuals Regarding the Automatic Processing of Personal Data
1986	UN Convention on the Rights of the Child
1990	United Nations Convention on Migrant Workers
1995	EU Data Protection Directive 95/46/EC 1999 African Charter on the Rights and Welfare of the Child
2002	African Union Principles on Freedom of Expression
2004	Arab Charter on Human Rights
2004	APEC Privacy Framework
2007	OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
2009	European Union Charter of Fundamental Rights
2010	Economic Community of West African States' Supplementary Act on data protection
2011	UN Guiding Principles on Business and Human Rights
2012	ASEAN Human Rights Declaration
2016	General Data Protection Regulation
2021	EU's preliminary AI Regulation
2022	EU's preliminary Digital Services Act

2023	EU's preliminary Directive on Corporate Sustainability Due Diligence

TABLE OF ABBREVIATIONS

ADHD	Attention-deficit/hyperactivity disorder
AICPA	American Institute of CPAs
Anr.	Another
APEC	Asia-Pacific Economic Cooperation
AR	Augmented Reality
ASEAN	Association of South East Asian Nations
BCI	Brain Computer Interface
CCPA	The California Consumer Privacy Act
CICA	Canadian Institute of Chartered Accountants
COPPA	Children's Online Privacy Protection Act
CPNI	Customer Proprietary Network Information
CPU	Central Processing Unit
ECG	Electrocardiography
ECHR	European Convention on Human Rights
ECPA	Electronics Communications Privacy Act
EEG	Electroencephalography
ECOSOC	Economic and Social Council
EMG	Electromyography
EU	European Union
FAQ	Frequently Asked Questions
FERPA	Family Educational Rights and Privacy Act

FTC	Federal Trade Commission
GAPP	Generally Accepted Privacy Principles
GB	Gigabytes
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSR	Galvanic Skin Response
HIPAA	Health Information Portability and Accountability Act
HMD	Head Mounted Display
HUP	Harvard University Press
IAPP	International Association of Privacy Professionals
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic Social and Cultural Rights
ID	Identity Document
IMU	Inertial Measurement Unit
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Right
IR	Infrared Radiation
ISP	Internet Service Providers
IT	Information Technology
LCD	Liquid Crystal Display
LED	Light-emitting diode
LGBTQ	Lesbian, Gay, Bisexual, Transgender, Queer
MR	Mixed Reality

MRI	Magnetic resonance imaging
NIST	National Institute of Standards and Technology
OASIS	Ontologically Anthropocentric Sensory Immersive Simulation
OECD	Organisation for Economic Co-operation and Development
Ors.	Others
OSCOLA	Oxford Standard for Citation of Legal Authorities
PSVR	Play Station Virtual Reality
Retd.	Retired
SCC	Supreme Court Cases
SCR	Supreme Court Record
SLAM	Simultaneous Location and Mapping
UDHR	United Nations Declaration of Human Rights
UIDAI	Unique Identification Authority of India
UN	United Nations
UNGA	United Nations General Assembly
UNDP	United Nations Development Programmes
UK	United Kingdom
UOI	Union of India
US	United States
USA	United States of America
v.	Versus
VNI	Visual Networking Index
VR	Virtual Reality
WCPSA	Wireless Communication and Public Safety Act

WWII	World War II
XR	Extended Reality
2D	Two Dimensional
3D	Three Dimensional
3DoF	Three degrees of freedom
6DoF	Six degrees of freedom
%	Percentage

CHAPTER 1

INTRODUCTION

1.1. RESEARCH BACKGROUND

The concept of the 'Metaverse' has gained considerable prominence and global recognition in contemporary times among the Individuals who exhibit a remarkable degree of competence in technology and exhibit a marked propensity to integrate state-of-the-art technological advancements into their daily practices. The proposed idea involves the creation of a new version of the Internet that would enable the establishment of an artificial digital realm or domain. The proposed digital domain is envisioned as a comprehensive platform that would enable individuals to engage in a diverse array of activities, such as professional endeavors, recreational gaming, e-commerce, social networking, and creative expression, among others. These activities would be seamlessly integrated into a unified virtual environment making it possible to analyze the structure of a virtual environment that pertains to individuals. However, the topic of establishing a digital environment is marked by considerable uncertainties and scholarly debates. The digital environment such as the Metaverse is a virtual environment that provides an immersive experience through the utilization of immersive technology and which has been conceptualized by big technology firms like Meta. The employment of immersive hardware is an essential requirement for individuals to participate in VR exploration, avatar generation, and user engagement. The concept previously mentioned exhibits resemblances to the simulated reality referred to as the 'Oasis,' as depicted in the literary work 'Ready Player One' penned by Ernest Cline.

The notion of the 'metaverse' is perceived by some as a convergence of the physical and virtual domains, whereby the material world is enhanced by digital interfaces and entities. The notion of a "metaverse" can be illustrated through the implementation of AR, as evidenced in applications such as Google Lens and the mobile game Pokemon Go. These technological advancements facilitate the ability of users to discover and engage with virtual depictions of Pokemon creatures situated within authentic physical surroundings. Currently, the metaverse is a commercial venture that is swiftly being constructed by major corporations in the gaming and technology industries, including Facebook, Apple, Google, and Microsoft. These companies are engaged in direct competition and allocate a significant portion of their technological resources towards developing their own designs for the metaverse. The scenario holds significant implications for society as it was evident by the transformative power of the

internet, the forthcoming iteration of our digital world is poised to have a profound impact on society. This impact will extend to the delivery of more engaging entertainment and more efficient commercial facilities, with far-reaching effects. The potential impact of such digital domain as metaverse extends beyond the realm of technological interaction, as it has the capacity to transform human behavior and societal dynamics. This raises significant questions regarding the influence of the metaverse on individual and national identities, particularly in a society where a substantial portion of the population may be engaged in parallel world interactions.

This discussion prompts us to delve into our subsequent investigation: what is the functional mechanism of the metaverse? Unfortunately, the functional mechanisms of the metaverse have yet to be clearly defined and at present stage, the software is in the beta phase and is undergoing additional development. Let us examine the beta phase of the software in greater detail in order to better understand its mechanism. During the beta phase, it is observed that users of such technology as metaverse will be granted access to an integrated digital ecosystem through a singular avatar or digital identity. This ecosystem is anticipated to possess its own currency, property, and possessions, thereby creating a digitally altered reality that can be likened to a VR. This VR may be constructed entirely from scratch or may be a hybrid of both reality and virtual elements. In the digital ecosystem such as the metaverse, users can utilize their avatars or digital identities to execute various online tasks that are currently dispersed across multiple digital properties, including websites and applications. This eliminates the necessity for passwords and user accounts that are presently associated with digital experiences. An instance of a Chinese social messaging application, WeChat, has achieved noteworthy interoperability by incorporating a discussion platform, payment system, and a social credit mechanism.[1]

Furthermore, it can be observed that gaming communities, such as Fortnite, meet the criteria of a prototype beta staged metaverse. The game boasts a global user base of 350 million registered individuals and features an internal monetary system that facilitates earning and trading of in-game currency.[2] The current state of the metaverse is characterized by the presence of building blocks that have not yet been integrated into a cohesive whole. Our understanding of this phenomenon is predicated on pre-existing knowledge and behavior. It

[1] Masha Borak, 'China's social app to rule them all wants to judge you for your purchases' (*South China Morning Post,* 11 January 2019) < https://www.scmp.com/abacus/tech/article/3029094/chinas-social-app-rule-them-all-wants-judge-you-your-purchases> accessed 18 May 2023.

[2] 'Registered users of Fortnite worldwide from August 2017 to May 2020' (*Statista,* 4 Jan 2023) <https://www.statista.com/statistics/746230/fortnite-players/> accessed 18 May 2023.

can be posited that while numerous prognostications may come to fruition, a plethora of alternative trajectories will inevitably falter and remain unexplored by both technological innovators and consumers. This is because technology evolves in tandem with human agency, as individuals aid in shaping its potentialities through adaptation and utilization.

In addition, a pivotal aspect of the metaverse concerns the diverse methods of entry. Presently, it is noted that achieving all-encompassing accessibility to the metaverse remains a challenging goal. The forthcoming matter of metaverse accessibility is anticipated to denote a noteworthy progression in the metaverse's beta phase. The present inquiry concerns the accessibility of the tool, with a specific focus on whether it will be made available through an open access framework or if it will adopt a commercialized approach with limited access.

Currently, individuals employ electronic devices, such as smartphones and laptops that are equipped with displays, to access the digital domain. The metaverse will enable individuals to enter the digital realm through a range of portable and immersive technological devices, such as HMDs, haptic gloves, wristwatches, and ocular contact lenses. Facilitating the engagement of individuals with a digital environment by means of various sensory channels, such as visual, auditory, and tactile modalities, instead of relying solely on a 2D display, has the potential to augment their perceptual and engagement capabilities within the digital ecosystem. The implementation of this specific class of immersive technology hardware will enable users to obtain improved and expedited access to the metaverse. The incorporation of this hardware will facilitate the acquisition of intricate and ever-changing user information through advanced algorithms, covering a range of metrics such as cardiac rhythm, dilation of the pupils, bodily movements, and the direction of visual focus.

As a result, this enables improved user access to the digital domain through a metaverse, in which providers of goods and services will have a deeper understanding of users' beliefs, concerns, and goals. In addition, extant data such as user preferences, engagement metrics, and social media interactions have already been in circulation and are leveraged by diverse platform providers to influence our digital encounters, market products and services to us, and exchange our personal information with third-party entities.

The development of the metaverse, driven by profit motives, poses a significant challenge in resisting the temptation to subject users to heightened levels of constant and detailed surveillance by the involved technology companies. Thus, the current issue presents a crucial question regarding the ownership and administration of the metaverse. The inquiry into the

ownership and governance of the metaverse is a subject that has piqued the interest of scholars. It is essential to investigate the parties that hold ownership over the metaverse's rights and those that will assume responsibility for its governance.

As previously mentioned, the lack of a completely functional virtual world or metaverse poses difficulties, if not insurmountable obstacles, in offering conclusive answers to the questions. Several prominent technology companies are endeavoring to function as portals or gateways to the metaverse. Everyone is striving to provide the best, if not the sole means of access.

Meta, formerly known as Facebook, has allocated a significant amount of funds, specifically $10 billion,[3] towards the development of its metaverse initiatives after its acquisition of Oculus Vision Tech, a company specializing in the production of immersive technology hardware, in 2014. Several prominent corporations, including Meta, Walmart, and Nike, have already taken measures to secure trademark protection and copyright for their virtual product offerings within the metaverse. It is highly probable that large corporations will endeavor to establish supremacy in the metaverse and safeguard their IPRs. However, this results in an unchallenged monopoly and poses significant issues as users of the metaverse will be fully immersed in a digital ecosystem that is shaped by major technology firms and large corporations. Consequently, interactions within this ecosystem will primarily occur in tandem with the rules and conditions put forth by these entities. Certain authoritarian regimes might develop metaverses that enable them to exert control over users by regulating content and access within these virtual environments.

Moreover, there exist concerns regarding the potential for a significant accumulation of wealth among a selected group of technology corporations who may leverage their privileged access to information to gain an unjust “first mover” advantage within the metaverse market. If the development of the metaverse is driven by commercial interests, there is a potential for prioritizing profit and consumer experience over activities that serve the greater good of society. Therefore, in order to ensure fairness and enable the metaverse to serve as a technological innovation that positively impacts human existence, it is imperative that digital domains such as the metaverse be accessible to all individuals and subject to oversight by an international regulatory body operating under the auspices of entities like EU and UN. This

[3] Jacob Kastrenakes and Alex Heath, ‘Facebook is spending at least $10 billion this year on its metaverse division’ (*The Verge*, 26 October, 2021) < https://www.theverge.com/2021/10/25/22745381/facebook-reality-labs-10-billion-metaverse> accessed 18 May 2023.

would allow for a diverse range of stakeholders to participate in the design of the digital ecosystem and ensure that it is regulated from its inception to uphold the rights of users.

Regulation of digital environment within the metaverse is a crucial aspect that requires careful consideration. The present challenge lies in the continued advancement of the ultimate architecture of the metaverse, which is presently in its beta phase. At present, there is a lack of precise understanding regarding the specific structure that will be adopted by the metaverse. The capacity to anticipate rapid technological advancements is of paramount importance for diverse entities, including governmental bodies, private enterprises, international institutions, and the broader society. Hence, the active involvement of stakeholders in collaborative initiatives aimed at establishing a regulatory framework that promotes an informed, worldwide, collaborative consensus to counteract the profit-driven interests of corporations is of paramount importance.

The development of such regulations requires the examination of various legal and human rights aspects. These factors include, but are not limited to, the extent of surveillance, information collection, and surreptitious promotion that is acceptable, as well as the safeguarding of vulnerable populations, such as underage individuals. In addition, there exist several technical factors that must be considered, such as adherence to contractual commitments, protection of intellectual property, determination of content ownership and licencing, and the transfer of digital resources.

The regulatory framework necessitates a proactive approach by governmental bodies, as opposed to the initial strategy employed during the nascent phases of the internet and social media. The regulatory framework must priorities endowing users with greater control and shift away from the current practice of surveillance capitalism, which relies on self-regulation by companies based on their own ethical principles and behavioral standards.

Concurrently, it is essential that governmental regulations maintain proportionality and adhere to established international human rights laws, which encompass the entitlement to freedom of expression. Preserving autonomy from governmental bodies is crucial for national regulatory agencies to prevent any potential occurrences of authority exploitation. An additional challenge pertains to the fact that policy makers lag technology firms, such as Meta, in their comprehension of the technological foundations of the metaverse, as well as its potential ramifications for commercial and other domains. The knowledge disparity gap also serves as a contributing factor to errors and omissions that have occurred over the past quarter-century.

Throughout this period, the governments enacted retroactive legislation in response to unforeseen issues, rather than proactively anticipating and addressing them. It is imperative that regulators possess a comprehensive comprehension of fundamental technological principles and refrain from operating in a state of obscurity. It is imperative for policymakers to establish proactive relationships with major technology companies and other enterprises to gain a deeper understanding of their objectives. This will enable them to identify potential societal risks and implement necessary regulations to address any gaps. The need for increased agility and predictability in digital regulations is paramount to mitigating the potential hazards that may arise from digital ecosystems like the metaverse. Failure to do so could result in the exacerbation of existing internet risks or the emergence of novel ones. The global community will be required to enhance its capacity to formulate legal frameworks that account for the swift advancements in technology. Governments may opt to modify current legislation or establish novel laws to effectively address the associated challenges. The cultural secretary of the United Kingdom has declared that the metaverse pursuits will be encompassed by the Online Safety Bill. It is probable that digital ecosystems, including the metaverse, will possess a transnational character for citizens across various nations. Therefore, it is imperative to establish international collaboration and synchronization regarding standards, as well as concerns such as competition and taxation. In addition, liberal democracies possess the potential to maintain their leading position in the regulation of guidelines or ethical standards for a conscientious metaverse. This would entail collaboration between governmental bodies and technology behemoths to integrate principles such as safety by design and privacy by design into their propositions for the metaverse.[4]

In addition, it is imperative that governments ensure that companies are held responsible for fulfilling their obligations in accordance with international human rights legislation, as outlined by the United Nations in its Guiding Principles on Business and Human Rights. In addition, it is imperative to implement measures such as due diligence and for technology companies to construct a digital ecosystem, such as metaverse architecture, that identifies potential risks during the design phase and endeavors to minimize those risks to the greatest extent possible. It is imperative that companies operating within the metaverse are held accountable for their activities, including data collection, algorithm usage, and transfer. Transparency regarding

[4] Harriet Moynihan, Marjorie Buchser, and Jon Wallace, 'What is the metaverse?' (*Chatham House,* 25 April 2022) <https://www.chathamhouse.org/2022/04/what-metaverse?gclid=Cj0KCQjwnMWkBhDLARIsAHBOftouWKQw7E-QNx2W1omWeEUcWIoCvmYjxQGsB1346RRAPmzMCjItVXgaAu-REALw_wcB> accessed 17 May 2023.

these practices is crucial, and companies should be held responsible for any harmful events that may occur. The implementation of such measures ought to be directed by the formulation of regulations by the European Union and national governments, for example, Digital Services Act of EU; its AI Regulation, and preliminary Directive on areas like Corporate Sustainability and Due Diligence. If these measures get implemented correctly, they could establish a universal international standard for democratic nations to adhere to.

Moreover, it is imperative to adequately address the critiques of the metaverse. The legitimacy of creating the metaverse or implementing regulatory measures to oversee its technical progress would be called into question if it were entirely characterized by negative aspects. Individuals have the ability to obstruct the progress of a specific technology, hindering its legitimate and transparent utilization, and instead preserving its covert nature similar to that of the Dark and Deep web, which is not readily accessible to the general public. But, the presence of the metaverse serves as evidence of its innovative nature, potentially yielding advancements across various societal domains beyond the realms of gaming and healthcare. The potential benefits of the metaverse extend to various domains, including healthcare, education, commerce, and creative industries. In certain instances, alternative methods may prove to be more effective than the internet. Like the internet, the metaverse presents an opportunity to enable knowledge sharing. The algorithms utilized in the metaverse have the potential to be designed in a manner that allows for learning from children's behavior. This can lead to the discovery of more effective teaching styles and learning spaces, both in virtual and physical environments. Consequently, this can enhance the interactivity of the learning process, reducing its passivity. In addition, the metaverse is poised to generate novel opportunities for recreational activities and artistic expression, affording users the ability to fashion their own distinctive realms and to reconfigure the physical world by adorning it with digital artwork and introducing novel varieties of virtual creatures to enhance their experiential encounters. Thus, Analogous to the internet, the metaverse holds promise for conferring substantial benefits in specific areas, while concurrently possessing the capability to considerably amplify pre-existing societal challenges. The widespread phenomenon of Internet surveillance conducted by both governmental and corporate bodies has been widely recognized for having blatant disregard for civil liberties, individual autonomy, and privacy.

Additionally, it can be argued that social media platforms have contributed to the exacerbation of polarization through the propagation of misinformation and the creation of echo chambers that shield users from opposing viewpoints. Under the surveillance capitalism paradigm, social

media platforms facilitate the transmission of user data to third-party entities that engage in targeted marketing or ideological messaging. It is a commonly observed phenomenon that after visiting product websites, advertisements for the same product are often exhibited on the individual's social media platforms. In addition, it is common for individuals to be uninformed regarding the collection, sale, or targeted marketing of their personal data on the internet, based on their browsing history or other personal information. The act of online manipulation has the potential to impede upon the liberty of cognitive processes, as evidenced by the Facebook-Cambridge Analytica scandal. This incident involved allegations that the data company Cambridge Analytica extracted information from the accounts of millions of Facebook users, with the intention of utilizing it for the purpose of promoting the candidacy of Donald Trump during the United States Presidential Elections. Consequently, it fosters a dichotomy of perspectives, insular communities, and heightened skepticism towards information outlets. Moreover, it is worth noting that Facebook is under the ownership of Meta, a prominent technology enterprise that is actively engaged in the advancement of metaverse technology. Therefore, there is a question as to whether the emergence of a digital ecosystem like the metaverse could exacerbate existing issues and give rise to novel challenges.[5]

The study's importance lies in its capacity to tackle a fundamental inquiry. Are there any prospective obstacles or hindrances linked to the notion of the metaverse? Regarding this inquiry, it can be argued that the main issue concerning the metaverse is its development being primarily motivated by commercial interests, with a lack of public discussion regarding essential considerations surrounding the desired structure of our upcoming digital environment. By whom should the design be undertaken? What should be the designated purpose and regulatory standards for its operation? Apart from the previously discussed human rights concerns, the metaverse presents additional potential societal risks, including the possibility of heightened digital exclusion. The unequal distribution of technologies necessary for participation in the metaverse is a prevalent issue affecting numerous individuals worldwide. In addition, there exist additional potential risks, such as the addictive properties of the metaverse, which could exacerbate mental health concerns and impede individuals' ability to sustain a fulfilling existence in the physical world outside of the metaverse domain. Moreover, the provision of highly personalized and automated services to cater to user preferences may exacerbate negative behaviors, including but not limited to the propagation of conspiracy theories, engagement in radical political activities such as trolling, and participation in

[5] Ibid.

gambling. Additionally, it is possible for Metaverse users to retreat into insular interest-based communities, potentially resulting in the emergence of a "splinternet" characterized by distinct digital ecosystems that are subject to national boundaries and control. In digital ecosystems that are fragmented, cultural perspectives may become more tribalistic, leading users to potentially disengage from reality and exhibit heightened hostility towards opposing viewpoints. The internet is the most valuable resource for the world's preparation towards the metaverse. The emergence of tech giants, insufficient regulation of the internet community, and the detrimental impact of social media behavioral patterns (algorithms) on democratic public discourse and opinions serve as valuable lessons for policy makers. In addition, there is presently an increased recognition of the issues that arise from the growing dominance of large technology corporations, akin to the opposition faced by major oil, pharmaceutical, and tobacco enterprises on a global scale. Presently, there exists an augmented comprehension regarding the significant harm inflicted upon society due to a reluctance to cease malevolent online conduct. Consequently, there is a need to consider protective measures considering this progress. Hence, the importance of this research lies in its emphasis on safeguarding the privacy, security, and data protection of individuals in the digital realm. Despite the current lack of attention and prioritization by global leaders, the study of privacy and data security issues in the digital ecosystem of Metaverse is crucial. Neglecting this issue, much like the neglect of climate change and pandemic prevention, could have significant consequences for humanity. Therefore, this paper aims to address the human rights concerning Right to Privacy and Data Protection by conducting research on the privacy and security concerns in Metaverse. This research seeks to fill the current gap in knowledge and contribute to the global effort to address this imminent challenge.

1.2. STATEMENT OF PROBLEM

As explicated in Section 1.1, the current digital environment, which encompasses the metaverse, presents numerous obstacles, such as the prevalence of profit-driven motives that guide its advancement. As has been noted, prominent corporations such as Walmart and Nike are presently pursuing trademark protection and copyright for virtual depictions of their merchandise within the metaverse, with the aim of asserting dominance in the digital realm and potentially achieving a monopolistic hold on the industry. This development raises significant concerns regarding the potential for engaging in anti-competitive behavior and the associated challenges. As a result, the metaverse would undergo a metamorphosis into a digital realm that is shaped and supervised by prominent technology enterprises and other substantial

corporations, with regulations and directives that are formulated according to their own stipulations and provisions. The potential outcome of this scenario is the formation of an autocratic government formed/influenced by such corporations which will enforce a unique type of authority over individuals by prescribing their decisions and violating their confidentiality and information on the World Wide Web. The ascendancy of prominent technology enterprises and corporations within the digital sphere, specifically in the metaverse, could potentially lead to a prioritization of financial gain and consumer satisfaction at the expense of the broader advantages offered by the digital ecosystem, including the metaverse, to society. Thus, it is imperative that policymakers from various liberal democracies and international institutions prioritize the development of regulations aimed at safeguarding the privacy and data protection of users within digital ecosystems.

Furthermore, as elucidated in Section 1.1, the science fiction film 'Ready Player One' which presents a comprehensive depiction of a digital ecosystem, denoted as 'OASIS' which refers to a virtual realm that is designed by the enterprise 'Gregarious Games,' established by James Halliday and Ogden Morrow, two scientists who devised the technology. As already mentioned, the 'OASIS' is a virtual reality platform that appeals to individuals from various socio-economic backgrounds, allowing them to participate in an alternative reality by means of avatars. Upon analyzing the literary work or cinematic rendition, it becomes apparent that the alternate universes hold greater importance than the physical reality. In addition, a multitude of prominent enterprises acknowledge the OASIS as a significant economic resource capable of yielding considerable financial gains, even to the point of breaching ethical boundaries. Following the demise of the 'OASIS' founder in the movie, a state of utter disorder ensues in the succession process, as the owner before his death programs and initiates an inheritance game. This game attracts the participation of major corporations, who deploy their finest resources to acquire 'OASIS' and gain control over this highly successful digital economic asset. Thus, depicting the primary objective of the big tech firms and corporations, which is to accumulate data on individuals in order to subsequently influence their decision-making processes and ultimately lead to greater profits. The game of inheritance in 'Ready Player One' reveals the unethical practices of large corporations as they violate various human rights. Hence, the paramount significance of safeguarding human rights pertaining to privacy and preventing any form of aggression towards other individuals is emphasized in the movie and in turn it underscores the necessity of intervention by international organizations and national governments to oversee the operations of an alternative digital ecosystem so that big tech firms

and corporations does not violate the Right to Privacy by breaching the privacy and collecting data of the users of Immersive Technology.

1.3. DETAILED LITERATURE REVIEW

The researcher has referred to several articles, books, and websites for this study on 'Understanding the Impact of Immersive Technology on The Human Rights Attitudes with Emphasis on Privacy and Data Protection Laws.' However, some of the articles and books made the basis of the research, without which the research would have been impossible. They are discussed in detail as follows:

Britanny Heller's article Reimagining Reality: Human Rights and Immersive Technology'[6] writes about the implications of Human Rights on Immersive Technology. In the article, Heller discusses the working mechanism of Immersive Technologies such as VR and AR. Furthermore, she also discusses the Immersive technology's role on society, the psychological impact of immersive experiences, and the content-based aspects of immersive experiences. She also talks in detail about the necessity for safety features inside such Immersive Experiences, explicitly focusing on the Biometric laws and the concept she called "Biometric Psychography" and its implications on Human Rights. Thus, the article by Heller provided the researcher with an idea of immersive technology and its operation mechanism and the knowledge of issues and challenges concerning privacy associated with immersive experiences, especially concerning Biometric Data. Finally, the article by Heller also guided the researcher with some solutions for safeguarding human rights inside the digital environment, accessed through immersive technologies.

Ellysse Dick, in her article 'Risks and Challenges for Inclusive and Equitable Immersive Experiences,'[7] talks about the potential of AR/VR in making services more inclusive and equitable in both the digital and non-digital. Dick further notes in the article that to achieve such goals, policymakers and industrialists must take steps to mitigate harmful impact of such technologies. Moreover, Dick also mentions in the article the risks and challenges marginalized or underserved communities face when using immersive technologies and talks about how offline bases tend to manifest in digital realms. Dick further stresses that to address this

[6] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf >

[7] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/>

challenge; it is stakeholders of AR/VR who should investigate issues such as privacy, discrimination, health, and harassment. Furthermore, Dick also mentions the unique issues of accessibility which are faced by disabled people in virtual spaces and people with poor broadband connections, affording capacity or digital illiteracy. Dick finally his article by stating that tech firms should design immersive experiences by considering a wide range of needs and preferences of the users of Immersive technology, such as the inclusion of different user controls and avatar-making to safeguard the privacy and integrity of the users. Thus, by going through the article by Dick, the researcher could understand the various challenges associated with Immersive Technologies, such as safety, inclusivity, and accessibility issues. Moreover, by referring to the article by Dick, the researcher also gets an idea to address the issue of inclusivity by tackling bias and discrimination and then the issue of accessibility faced by disabled and poor people.

Ellysse Dick, in her article 'Balancing user privacy and innovation in Augmented and Virtual Reality,'[8] stated that the AR/VR devices create numerous issues related to privacy in immersive expediencies due to the scope, scale and sensitivity of the information collected for such experiences. Hence, he states in the article that to mitigate such forms of harm, it is the duty of the policymaker to reform the regulatory framework of data privacy in Immersive technology, which is currently failing to address some risks while also over-regulating in response to other issues. Dick starts the article by explaining how AR/VR devices collect data similarly to other consumer technologies and raise an issue related to the privacy and sensitivity of the information collected by such devices. Dick further discusses the collection of extensive biometric data and the privacy risks due to such collection. Moreover, dick states that due to the immersive nature of AR/VR, it is difficult to mitigate the risk by applying the policies and practices related to privacy from other digital media and requires an innovative approach providing transparency, choice, and security. Furthermore, Dick also argues that regulating the AR/VR or immersive technologies used for accessing immersive experiences is leaving the current legal policies a step behind innovations and is constantly evolving; thus, the policymakers should regulate based on actual harms associated with user data and should start creating an innovation-friendly environment for regulating the privacy of the users of Immersive Technologies in AR/VR by clarifying, updating and harmonizing existing rules and introducing comprehensive privacy legislation within nations. Thus, after referring to this

[8] Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/>

article by Dick, the researcher could figure out the various issues and challenges associated with privacy and data concerning immersive experiences and the types of Data monitored. Furthermore, by referring to the article, the researcher could also figure out some measures by referring to the lacunae in existing regulatory mechanisms dealing with privacy and data protection inside immersive experiences.

Ernest Cline, in his novel 'Ready Player One',[9] narrates the story of an artificially created virtual reality called OASIS and the challenges and issues which prevail in the OASIS due to the commercial interest of tech companies to win the game of inheriting the OASIS. This novel helped the author to picture a world in the metaverse and, in turn, understand the complexities and issues related to privacy and data protection in such a world.

Ellysse Dick, in her article 'How to address privacy questions raised by the expansion of Augmented Reality in Public Spaces,'[10] states that the AR amplifies the privacy concerns for bystanders in the virtual realm and combines them in novel ways. Dick states that policymakers should develop safeguards to shift perceptions of privacy in public spaces. Furthermore, by referring to the article by Dick, the researcher figures out that privacy concerns associated with individuals are not unique to AR but seen in other digital technologies, and it is just the AR that amplifies the already existing privacy issues due to digital technologies for bystanders. Moreover, the researcher also finds out, after referring to the article by Dick, that the critical policy challenges associated with privacy due to the various digital technologies also apply to AR. Further in the article, Dick also states that the potential of AR/VR devices to collect, analyze and display personal data in real-time challenges the existing norms, and more adoption of such devices will make it necessary to make changes in the social and legal definition of privacy and to establish guidelines for using AR by law enforcement bodies to address surveillance issues. Dick further states that lawmakers should not create unique laws for AR devices and services and instead should facilitate the development of voluntary standards, best practices, and codes of conduct to protect bystanders' privacy. Thus, the researcher learns from this article that along with making stringent laws to deal with privacy issues in Immersive experiences, it is also important to make the users of immersive technologies morally strong to operate in a manner that does not violate each other's rights in

[9] Ernest Cline, *Ready Player One* (Cornerstone, 2012).
[10] Ellysse Dick, 'How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces' (*Information Technology and Innovation Foundation,* 14 December 2021) <https://itif.org/person/ellysse-dick.>

the virtual realms and facilitated standards and practices which protects and protects the privacy of a bystander.

The publication 'Privacy and the Indian Supreme Court'[11] by NLU Delhi (Centre for Communication Governance) is a publication which deals with a detailed analysis of the Supreme Court of India's privacy jurisprudence during the last 70 years. The publication discussed in detail the various cases associated with Privacy Jurisprudence in India, such as A.K. Gopalan v. State of Madras, Justice K.S. Puttaswamy v. Union of India, Kharak Singh v. State of Uttar Pradesh, Maneka Gandhi v. Union of India, M.P. Sharma v. Satish Chandra, District Magistrate, Delhi, and Rustom Cavasji Cooper v. Union of India. This publication made the researcher understand the Indian privacy jurisprudence with the help of essential case laws of India.

In his book 'Data Protection Law in India,'[12] Pavan Duggal dealt with and discussed in detail the Data Protection basics and the principles of Data Protection, which is in application Internationally and nationally in countries such as the USA, UK, Australia, China and India. The researcher has repeatedly referred to the book to understand Data Protection and its principles. Moreover, the researcher has solely relied on this book to understand and explain the concepts of Data Protection and refer to various data protection laws of countries such as the US, UK, Australia, China, and India.

Lisa S. Nelson, in her book 'America Identified-Biometric Technology and Society,'[13] dealt in detail with the perception of biometric technology among the public regarding privacy, security, and civil liberties. Lisa, in her book, investigated the public perception of biometric technology to explore values, beliefs and ideologies that affect public acceptance of the technology. This book made the researcher understand the importance of learning about Biometric laws in correlation to immersive experiences. Most of the researcher's knowledge about Biometric laws and the current legal scenario dealing with privacy and data protection associated with Biometric Data within immersive experiences of the digital realm comes from reading articles by Brittan Heller and Ellysse Dick. However, after referring to the book by Lisa, the researcher further understood the impact and importance of having stringent, calculative, and researched

[11] Krishna Prasad S, 'Privacy and the Indian Supreme Court' National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf >
[12] Pavan Duggal, *Data Protection Law in India* (Universal Law Publishing, 2016).
[13] Lisa S. Nelson, *America Identified-Biometric Technology and Society* (The MIT Press, 2010).

legislation of Biometric laws both nationally and internationally and the awareness among the public about the potential threat which Biometric Data carries.

Danielle Keats Citron, in his book 'Hate Crimes in Cyberspace,'[14] discusses in detail the various extents of personal cyber-attacks and the measures to prevent & punish such forms of online harassment. Further in this, Citron reveals the seriousness, emotional damage, and financial & professional harms incurred by victims due to crimes in cyberspace. He also states how such crimes often target vulnerable victims and harass them; therefore, legal measures and social norms must to taken together to deal with such issues. This book makes the researcher understand the various forms of crimes inside cyberspace and the forms of violence and crimes that might happen inside cyberspace accessed through immersive technologies.

1.4. AIMS

This research aims to explore the topic of human rights by analyzing the privacy and data protection obstacles linked to the digital ecosystems that can be accessed through Immersive Technologies. The research mainly aims at understanding the working mechanism of immersive technologies and addressing challenges and issues faced under Immersive Technologies and the current gaps in law dealing with the issues of privacy and data protection concerning immersive technologies. The research also aims to discuss primarily a vital aspect of Biometric Privacy which is an essential aspect of Privacy and Data Protection under Immersive Technologies. Furthermore, the research seeks to figure out a feasible solution to the challenges in immersive experiences, such as safety, inclusivity, accessibility and the issue of Privacy and Data Protection in digital environments accessed through immersive technologies.

1.5. OBJECTIVES

As discussed, this research paper aims to determine the challenges of using Immersive Technology regarding safety, inclusivity, and accessibility. Furthermore, the research paper also seeks to inquire about the Privacy and Data Protection issues of the users of Immersive Technology from the commercial interests of large technology companies and third parties involved in its development. Thus, the research paper has the following objectives:

1. To understand Immersive technology and its mechanism of operation.
2. To understand the societal ramifications of Immersive Technology on its users.

[14] Citron D, *Hate Crimes in Cyberspace* (1st edn, HUP 2014).

3. To figure out the challenges encountered within the domain of digital environment accessed through Immersive Technology, such as safety, inclusivity, and accessibility.
4. To figure out the current state of privacy and data protection in the context of immersive technology and its impact on human rights.
5. To figure out the potential solutions for addressing privacy and data protection concerns in the context of immersive technology.

1.6. SCOPE AND LIMITATIONS

The scope of this paper is limited to the study of human rights issues associated with immersive technologies, with a particular focus on the issues of Privacy and Data Protection in Immersive technology due to the commercial interests of big tech firms and corporations in Immersive technology.

Due to the novel nature of the research, the author faced limitations regarding the availability of resources and literature in the library. Thus, the author had to rely mainly on the limited online resources available to conduct a comprehensive study on the topic 'of understanding the impact of immersive technology on human rights attitudes with an emphasis on privacy and data protection laws.

1.7. RESEARCH QUESTIONS

As discussed in the introduction, many users use Immersive Technology for utility purposes, such as gaming, recreation, etc., making immersive technology an exciting technology for everyday use. However, this technology and such utility purpose bring several challenges, such as safety, inclusivity and threats to privacy and data protection within the digital spaces accessed through immersive technologies. Hence the researcher has formulated the following research questions:

1. What is the meaning of the term 'Immersive technology'?
2. What is the operation mechanism of the 'immersive technology'?
3. What are the societal ramifications of Immersive Technology on its users?
4. What challenges are encountered within the digital environment domain accessed through Immersive Technology, such as safety, inclusivity, and accessibility?
5. What is the current state of privacy and data protection in the context of immersive technology and its impact on human rights?
6. What are the potential solutions for addressing privacy and data protection concerns in the context of immersive technology?

1.8. RESEARCH METHODS

This study represents an applied legal research project to address the practical issue of privacy and data breaches in Immersive Technologies. This research utilized the doctrinal approach and primarily relied on online articles as its primary data source. The predominant sources employed for this study comprise secondary sources, particularly articles and books. The current study is qualitative legal research that significantly emphasizes the qualitative aspect while refraining from integrating any quantitative analysis. The study in question has been referenced using the fourth edition of OSCOLA.

1.9. RESEARCH DESIGN

1. Introduction

The chapter will highlight the prospective transformative impacts of the metaverse on the interplay between humans and technology and the broader association between humans and their environment.

2. Understanding Immersive Technology

In the subsequent chapter about Immersive Technology, the researcher has determined that the technology is currently in a nascent stage of development. Furthermore, the devices required to access this technology are also undergoing development. Most of these devices are subject to scrutiny due to their origin from large private technology firms and corporations whose primary objective is the practice of surveillance capitalism. Moreover, the author has also discussed the challenges Immersive Technologies face in this chapter.

3. Privacy & Data Protection in Immersive Technologies

This chapter pertains to the topic of privacy. Within this chapter, the researcher has expounded upon the significance of the Right to Privacy and Data Protection as fundamental Human Rights, as recognized by both International Human Rights Law and National legislation, including that of India. Additionally, this chapter has discovered that immersive technology devices present new challenges regarding users' privacy because of the scope, scale, and sensitivity of the information they gather from users, which has been discussed in this chapter in detail. In order to address such risks associated with immersive technologies, it is thus recommended in the chapter that the regulators and policymakers reform the current regulatory mechanisms for data privacy.

4. Immersive Technology- A Way Forward

The study's concluding chapter revealed the potential of immersive technology, highlighting its prospects that may encompass sophisticated bodily movements, haptic or neurological interfaces, and pupil dilation hardware. The form of progress gives rise to the challenge of formulating 'biometric psychography,' which pertains to the amalgamation of behavioural and anatomical data that can utilize to recognize or quantify an individual's response to stimuli over a period which can be employed to gain an understanding of an individual's physiological, psychological, and emotional condition, as well as their preferences. Therefore, the study's findings suggest that using immersive technology by big tech firms and corporations for eye tracking and pupil dilation monitoring can reveal information beyond identity, which can have consequences on user privacy, human rights, and the potential for self-censorship.

5. Conclusion and Suggestions

In conclusion, the researcher asserts that the emergence of Immersive Technology constitutes a noteworthy progression for humankind. It is imperative to recognize that, akin to a coin, this innovation carries both favourable and unfavourable ramifications. Thus, it is crucial to incorporate safety protocols during the creation, implementation, and management of Immersive Technology to safeguard human rights matters such as freedom of expression, safety and security, privacy, and data protection, which should be regarded as a significant issue in the context of Immersive technology due to its potential impact on users' physical and mental well-being.

CHAPTER 2

UNDERSTANDING IMMERSIVE TECHNOLOGY

2.1. INTRODUCTION TO IMMERSIVE TECHNOLOGY

The concept of “immersive technology” pertains to technological devices that induce a feeling of immersion or presence, leading individuals to experience complete absorption in a digital or virtual environment. The concept encompasses a broad spectrum of technological advancements that strive to improve and amplify the user's cognitive abilities and engagement with the digital realm. Frequently, this entails the amalgamation of various sensory modalities, including but not limited to visual, auditory, and tactile perception. Immersive technology is a term that encompasses a variety of modalities, such as VR, AR, and MR, which are widely acknowledged as some of the most notable examples. VR refers to a technological innovation that generates a completely synthetic digital environment that replicates a genuine or imaginary setting. On average, individuals utilize a VR headset to fully immerse their visual and auditory senses, thereby facilitating a comprehensive 360-degree view of the simulated environment. The commonly used approach involves the use of portable controllers or sensors to track bodily movements, which facilitates user interaction and movement within the virtual environment. AR is a technological advancement that superimposes digital information onto the physical environment, creating a seamless integration of virtual and real-world elements. The technology of AR can be accessed through a range of devices, including smartphones, tablets, and smart glasses, which enables users to engage with this technology. AR is a technological advancement that amplifies the sensory perception of the user's tangible environment by superimposing computer-generated graphics, textual information, or other virtual elements onto the user's physical surroundings. The virtual components have been designed to demonstrate interactive and responsive behaviour in alignment with the user's surroundings. MR is an emerging technological innovation that combines the unique features of VR and AR to facilitate simultaneous interaction between virtual and real-world objects for users. The concept pertains to the integration of digital media with the tangible surroundings, enabling individuals to engage with computer-generated entities as if they were physically present in the real environment. The incorporation of sophisticated headsets or glasses is a widely used approach in this technological domain, enabling a smooth amalgamation of virtual and tangible components.

Such forms of Immersive technology have a diverse range of applications across multiple domains, such as entertainment, gaming, education, healthcare, architecture, engineering, and training simulations. The utilization of virtual reality technology presents distinctive prospects for the development of authentic and captivating experiences. This technological advancement facilitates the ability of individuals to partake in the exploration of novel environments, acquisition of fresh skills, and interaction with virtual entities and objects in manners that were previously unattainable.

Moreover, the emergence of immersive technology signifies a noteworthy technological progression, with various sectors such as healthcare, MedTech, defence, aerospace, and manufacturing, having already adopted XR as a mechanism for attaining significant advancements. Various industries are currently utilizing XR technology, which encompasses augmented, virtual, and mixed realities, to enhance their training and educational capabilities, improve visualization and modelling, optimize planning and production processes, and heighten safety and awareness protocols. Various estimations have been proposed with regards to the scale of the XR sector.

However, according to optimistic projections, the global XR sector is expected to reach a valuation of $1.1 trillion by the year 2030.[15] The projected expansion is expected to be driven by technological advancements and a broader consumer base. Furthermore, the implementation of immersive experiences has the potential to provide a variety of advantages to various stakeholders, contingent on their objectives and sector. As per conducted research, the incorporation of immersive technology for the purpose of employee training resulted in a noteworthy reduction in employee errors by approximately 40%.[16] According to Walmart's research findings, the integration of immersive experiences resulted in a noteworthy increase of 70% in the test scores of their employees.[17] The findings of recent inquiries have established a noteworthy increase of 29% in task performance speed among first responders after receiving VR training.[18] Empirical studies have indicated that immersive experiences have the potential

[15] 'Extended Reality [XR] Market' (*Transparency Market Research*) <https://www.transparencymarketresearch.com/extended-reality-xr-market.html> accessed 18 May 2023.
[16] Przemysław Zawadzki et al, 'Employee Training in an Intelligent Factory Using Virtual Reality' (2020) IEEEAccess <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9144168> accessed 18 May 2023.
[17] Sarah Fister Gale, 'Case study: Walmart embraces immersive learning' (*Chief Learning Officer,* 23 March 2021) <https://www.chieflearningofficer.com/2021/03/23/case-study-walmart-embraces-immersive-learning/> accessed 18 May 2023.
[18]George Koutitas, Scott Smith and Grayson Lawrence, 'Performance evaluation of AR/VR training technologies for EMS first responders' (2021) Springer <https://www.researchgate.net/publication/340415977_Performance_evaluation_of_ARVR_training_technologies_for_EMS_first_responders> accessed 18 May 2023.

to enhance students' concentration, comprehension, and knowledge retention in educational environments. Moreover, it has the potential to decrease the duration required to acquire knowledge or mastery.

Furthermore, as per the findings of Wiley's research, the utilization of AR projection technology resulted in a noteworthy decrease in the incidence of failures while inserting the liver biopsy needle with improved accuracy. Precisely, the percentage declined from 50% to 30%.[19] As per a recent research investigation, the implementation of VR oriented instruction has led to a significant 30% enhancement in academic achievement among children of various age groups. According to the research conducted by the National Training Laboratory, individuals who utilized virtual reality exhibited a retention rate of 75%,[20] which is significantly higher than the retention rates associated with reading and lectures, which were 10% and 5%, respectively. The incorporation of immersive experiences can serve as effective narrative tools to enhance consumer engagement. In addition, virtual experiences have the potential to improve brand and product perception, surmount the constraints of physical presence, and streamline the process of decision-making. Snap Inc., Alter Agents, and Publicis have reported an 80% rise in consumer decision-making confidence through the utilization of immersive technology.[21] According to Deloitte's research, the integration of on-site immersive AR experience enhancements resulted in a significant 30% increase in the number of physical customers visiting brick-and-mortar stores.

Nevertheless, a significant obstacle that needs to be surmounted prior to attaining broader recognition is the limitation of realism. Even though certain immersive headsets can presently attain a resolution that is akin to that of the human eye, further technological advancements are necessary to attain absolute photorealism in virtual encounters. XR technology has the capability to immerse users completely in simulated environments. However, a crucial challenge that demands consideration is the need for users to proficiently distinguish between

[19]Guido Makransky, Stefan Borre-Gude and Richard Mayer, 'Motivational and Cognitive Benefits of Training in Immersive Virtual Reality Based on Multiple Assessments' (2019) Wiley <https://www.researchgate.net/publication/333394912_Motivational_and_Cognitive_Benefits_of_Training_in_Immersive_Virtual_Reality_Based_on_Multiple_Assessments> accessed 20 May 2023.

[20]'How Virtual Reality is Transforming Education Tech and Training' (*CBINSIGHTS,* 15 December 2020) <https://www.cbinsights.com/research/virtual-reality-education-training tech/#:~:text=The%20National%20Training%20Laboratory%20found,like%20reduced%20errors%20and%20injuries> accessed 21 May 2023.

[21]'Exploring the utility of AR in Marketers' E-Commerce Plan' (*Snapchat,* 16 June 2022) <https://forbusiness.snapchat.com/blog/exploring-the-utility-of-ar-in-marketers-ecommerce-plan> accessed 22 May 2023.

the virtual and physical environment. Similarly, it is conceivable that some individuals may lack the necessary skills or resources to fully engage in immersive experiences.

Notwithstanding the growing ubiquity of immersive experiences and XR devices worldwide, which is projected to result in the distribution of approximately 50 million units of AR and VR headsets[22] in both consumer and commercial markets by 2026, the current rate of global adoption is insufficient to warrant such a classification. The advancement of XR technology is expected to result in the refinement and increased immersion of headset designs, as well as a reduction in their weight. The incorporation of XR devices into various domains such as work, education, collaboration, entertainment, and related areas can be expanded. It is expected that the intensification of competition in the endeavour to establish a presence in the consumer market, coupled with this specific trend, will lead to a decrease in the price of headsets, thereby addressing the concern of accessibility in the market. It is expected that the forthcoming generation of immersive devices will demonstrate noteworthy advancements in both their hardware and software components. It is anticipated that the incorporation of auto-focus functionality would provide a significant advantage, as it would emulate the natural focusing mechanism of the human eye. Incorporating a highlight dynamic range into XR technology has the potential to enhance the visual depth and realism of light-contrast-focused experiences. All these characteristic features were exhibited in the Meta Prototype Exhibition of 2022.[23]

Furthermore, the primary inquiry that persists is: What is the maximum velocity at which these characteristics can be amalgamated into a solitary headset? Simultaneously, it is anticipated that the realm of software will experience substantial progressions that align with the advancements in hardware capabilities. The resultant software output, derived from the provided experience, will play a crucial role in fulfilling the anticipated standards. The resulting output will encompass aspects such as visual precision, level of genuineness, interface design, and user engagement. Furthermore, the structural composition and operational capabilities of the hardware will also exert a substantial influence in attaining these benchmarks. Despite the widespread availability of immersive experiences that boast exceptional visual fidelity in

[22] Needham, 'AR/VR Headset Shipments Grew Dramatically in 2021, Thanks Largely to Meta's Strong Quest 2 Volumes, with Growth Forecast to Continue, according to IDC' (*IDC,* 21 March 2022) <https://www.idc.com/getdoc.jsp?containerId=prUS48969722> accessed 21 May 2023.

[23] Adi Robertson, 'Mark Zuckerberg has so many VR headset prototypes to show us and none of them are shipping' (*The Verge,* 20 June 2022) <https://www.theverge.com/2022/6/20/23172503/mark-zuckerberg-meta-vr-headset-prototype-reveal-butterscotch-sunburst-holocake-mirror-lake> accessed 21 May 2023.

contemporary times, it remains imperative to attain a level of realism that is commensurate with reality.

Currently, it is possible to generate digital replicas of nearly any object or entity, alongside immersive spatial audio and highly authentic avatars that can swiftly capture and convey emotions and facial expressions. It is anticipated that the forthcoming significant breakthrough will arise from the progression of haptic technology,[24] which has the potential to simulate tactile sensations for users, in conjunction with visual and auditory stimuli. Based on estimations, it is anticipated that the haptic technology industry will attain a minimum valuation of $23.8 billion by 2030.[25] If possible, the forthcoming sequence of immersive encounters will be remarkably remarkable with regards to their visual and sensory characteristics. The integration of haptic technology holds promise as a noteworthy advancement in the realm of immersive experiences. This can be attributed to its capacity to elicit stimulation across various sensory modalities and augment our extant comprehension of the world. The concept of "immersive" can be readily distinguished and delineated between genuine and artificial immersive encounters. It is expected that in the forthcoming years, immersive experiences will surpass current standards by exhibiting heightened sensory characteristics, hyper-realism, and near-perfect emulation of real-life interactions. But the adoption of such advanced technology is expected to present certain obstacles, including concerns related to privacy and data protection. Even though it is anticipated that this technology will yield substantial benefits for various sectors, businesses, and individual consumers this comes at the expense of an unregulated digital landscape, where various big tech firms and corporations may prioritize their commercial interests over safeguarding the fundamental human right of privacy and data protection.[26] Thus creating a challenge and gap in the International Human Rights Law and legal domain in general. But before discussing this challenges and gaps let us try to understand the mechanism behind the functioning of Immersive Technology.

[24] Alex Balladares, 'Understanding Haptics for VR' (*Virtual Reality Pop,* 3 May 2017) <https://virtualrealitypop.com/understanding-haptics-for-vr-2844ed2a1b2f> accessed 21 May 2023.
[25] 'Haptic Technology Market (By Component: Solution, Software; By Application: Consumer Electronics, Gaming, Healthcare, Robotics, Education, Research, Others; By Feedback Type: Tactile, Force) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2022-2030' (*Precedence Research,* September 2022) <https://www.precedenceresearch.com/haptic-technology-market> accessed 21 May 2023.
[26] Alex Dzyuba, 'Immersive Experience: The Definition, The Technology and the Future' (*Forbes,* 2 Jan 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/01/02/immersive-experience-the-definition-the-technology-and-the-future/?sh=304efd5f4e0d> accessed 23 May 2023.

2.2. THE MECHANISM BEHIND THE FUNCTIONING OF IMMERSIVE TECHNOLOGY

2.2.1. VR INTERFACES

Regarding its functionality, VR functions similarly to a combination of a motion picture and a View-Master, as used in the past. The HMD of a virtual reality VR headset showcases the computer processor's visual output, which may be either integrated within the HMD or situated externally. The HMD facilitates the transmission of two distinct visual streams to a pair of LCD screens, namely a left and a right screen, with each screen being designated for one eye. The HMD integrates additional lenses that are strategically placed between the display and the user's eyes, with the purpose of focusing the visual output. When an observer gazes through the viewfinder, their visual perception is directed through the lenses, leading to a stereoscopic interpretation of the tridimensional space. This phenomenon is accomplished through the nuanced discrepancies present between the images on the left and right. The phenomenon refers to the amalgamation of slightly disparate viewpoints perceived by the left and right eyes, which results in the creation of a sense of depth in one's visual perception.[27]

In general, a wider range of visual perception has been observed to increase the degree of immersion in an encounter. Most VR visual displays typically feature a field of view ranging from 100 to 110 degrees.[28] It is anticipated that cutting-edge hardware will integrate foveated rendering, a method that entails the obscuring of peripheral scenes, akin to the inherent occurrence of central focus and blurred peripheries in human visual perception. This Foveated rendering is a technique that utilizes ocular monitoring to optimize the rendering process.[29] To be more Specific, the HMD utilizes the user's pupils' location to determine which regions require high resolution and which regions can be rendered at a lower resolution.[30] The aforementioned methodology possesses the capability to preserve computational resources in the course of an interactive session, thus empowering developers to integrate more intricate levels of specificity within the designated area.[31]

---

[27] Zaynah Bhanji, 'A New Reality: How VR Actually Works' (*MEDIUM,* 2 Oct 2018) <https://medium.com/predict/a-new-reality-how-vr-actually-works663210bdff72> accessed 23 May 2023.
[28] 'Field of View for Virtual Reality Headsets Explained' (*VR LENS LAB*) <https://vr-lens-lab.com/field-of-view-for-virtual-reality-headsets/> accessed 23 May 2023.
[29] Jeremy Horwitz, 'HTC Vive Pro Eye hands-on: Gaze into VR's future with foveated rendering' (*VENTUREBEAT,* 10 January 2019) <https://venturebeat.com/business/htc-vive-pro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 23 May 2023.
[30] Ibid.
[31] Ibid.

HMDs employ sensors to track and document the user's motions, precisely ascertain their spatial position, and promptly modify their visual viewpoint. Moreover, the term "tracking" pertains to the ability of hardware to accurately measure and quantify a user's head and eye movements, and subsequently modify the user's perspective accordingly.[32] HMDs employ spatial mapping techniques to ascertain the position and rotation of the user's head. The precise monitoring of the user's head movements along the X, Y, and Z axes is accomplished via a mechanism referred to as six degrees of freedom. The axes denoted as X, Y, and Z are commonly referred to as orientation, position, and rotation, respectively. Consequently, the exhibited visual representation is adapted to align with the user's cranial motions, thereby facilitating a heightened sense of engagement.[33] The incorporation of optical and non-optical sensors facilitates the spatial localization of the human body, thereby reducing the likelihood of accidental self-harm or stumbling while engaged in an immersive encounter. The portable controllers or HMDs incorporate accelerometers, gyroscopes, and magnetometers to convert physical movement into electrical signals, which enables the tracking of motion.[34]

Furthermore, the process of hand tracking involves the utilization of optical sensors, which is presently undergoing swift development. Interfaces that lack controllers employ electrical signals to enable manipulation of VR software through gestures.[35] The integration of these sensors collectively enables the monitoring of the user's physical actions and behavior. The prompt reaction of hardware to user movements holds significant value in reducing latency and preventing users from experiencing discomfort while engaging in immersive experiences.

Moreover, the human perceptual system is a sophisticated mechanism that can be vulnerable to "simulation sickness" if the rendering, tracking, or display characteristics are not accurately calibrated. Also, it is to be noted that the term Latency refers to the duration of time that elapses between a user's head or eye movement and the corresponding change in their perspective.[36] In addition to visual delays, latency can encompass delays in other sensory perceptions as well. In order to mitigate the occurrence of nausea or disorientation among users, it is imperative to

---

[32] Jonathan Strickland, 'How Virtual Reality Works' (*Howstuffworks)* <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed 23 May 2023.

[33] 'A Quick Guide to Degrees of Freedom in Virtual Reality' (*Kei Studios,* 2018), <https://kei-studios.com/quick-guide-degrees-of-freedomvirtual-reality-vr/> accessed on 24 May 2023.

[34] 'Understanding Sensors: Magnetometers, Accelerometers and Gyroscopes' (*Virtual Reality Society,* 2017) <https://www.vrs.org.uk/virtual-reality-gear/motion-tracking/sensors.html> accessed on 23 May 2023.

[35] Meta Quest Blog, 'Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR' (*Meta,* 25 Sep 2019) <https://www.meta.com/blog/quest/introducing-hand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed on 24 May 2023.

[36]'Latency - Virtual Reality and Augmented Reality' (*VR AR & XR WIKI*) <https://xinreality.com/wiki/Latency> accessed on 24 May 2023.

ensure a minimum rendering rate of 60 frames per second when utilizing a HMD. Nevertheless, certain providers of content choose to offer an elevated frame rate in order to furnish an enhanced user experience.[37] The importance of this observation stems from the fact that humans exhibit an elevated sensitivity to latency, as indicated by findings from flight simulator studies that have illustrated our capacity to detect latency delays surpassing 50 milliseconds. Latency in immersive environments can result in an increased awareness of the artificiality of the environment, which can undermine the desired sense of an alternate reality.[38]

The importance of eye tracking within the context of VR is of great significance and will be elaborated upon in subsequent sections of this academic paper. In summary, the eye tracking process involves the utilization of an infrared camera to observe and monitor the gaze direction of a user within a HMD. The utilization of sensors yields improved precision in computational feedback within virtual reality content, culminating in a heightened sense of realism. As aforementioned, Foveated Rendering holds promise in augmenting visual verisimilitude through the blurring of peripheral vision edges, consequently diminishing the probability of inducing motion sickness.[39]

2.2.2. AR INTERFACES

AR can be differentiated from VR in that it superimposes computer-generated sensory inputs onto the physical surroundings. The apparatus in question utilizes a camera system and a computer that is integrated into a HMD to analyze a specific visual field and the respective object positions within it. Following this analysis, the apparatus superimposes visual representations or textual annotations onto the user's field of view.[40]

The application of AR features on mobile devices, utilizing a single camera and potentially a depth camera, can aid in the execution of SLAM through algorithmic methods. The integration of cameras with the accelerometer and gyroscope of a handheld device is a common practice,

---

[37] Jonathan Strickland, 'How Virtual Reality Works' (*Howstuffworks*) <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed 24 May 2023.
[38] Ibid.
[39] Jeremy Horwitz, 'HTC Vive Pro Eye hands-on: Gaze into VR's future with foveated rendering' (*Venturebeat,* 10 January 2019) <https://venturebeat.com/business/htc-vive-pro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 25 May 2023.
[40] Peggy Johnson, 'Spatial Computing: An Overview for out Techie Friends' (*Magic Leap,* 27 August 2018) <https://www.magicleap.com/blog-staging/spatial-computing-an-overview-for-our-techie friends#:~:text=Spatial%20computing%20is%20about%20volumes, access%20through%20Magic%20Leap%20One.> accessed 25 May 2023.

collectively known as an IMU. The SLAM algorithm incorporates multiple sensors to determine the spatial coordinates, orientation, and movement of the mobile device.[41]

HMDs that are currently used for XR applications utilize similar orientation techniques, but with added inputs that enable the overlay of digital content onto real-world environments. XR encompasses the collective set of both physical and virtual environments that are created through computer graphics and wearable technologies. The symbol 'X' within the context of XR represents a variable that possesses the ability to represent any letter within a given context. XR is a comprehensive classification encompassing diverse manifestations of computer-mediated reality, such as AR, MR, and VR. Rather than employing a single camera, a HMD will produce a depiction of its surroundings using multiple wide-angle cameras that often have lower resolutions and are positioned in various orientations. Eye tracking systems commonly employed in AR and XR applications comprise a camera that is oriented towards the user's eyes, with certain systems utilizing infrared light for functionality. In the past, older systems utilized a unique infrared light field that was generated by external "lighthouses" in combination with its internal IMU to deduce the user's position and orientation of movement.[42] Some AR systems, such as the Magic Leap, integrate a singular handheld device that is furnished with an increased quantity of integrated sensors.[43] On the contrary, systems such as the Microsoft HoloLens exclusively depend on manual input provided by the user's hand.[44]

The incorporation of AR camera and sensors leads to the formation of a self-reliant computational stratum, separate from the exhibition mechanism. After obtaining information about its positioning and alignment, the apparatus possesses the ability to produce a virtual 3D setting based on the user's perspective. Afterwards, the display system overlays the rendering onto the visual field of the observer.

---

[41] Jonathan Strickland, 'How Virtual Reality Works' (*Howstuffworks*) <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed on 25 May 2023.

[42] Jeff Suovanen et al, 'Magic Leap One Teardown' (*IFIXIT,* 23 August 2018) <https://bit.ly/2Z2Df4L> accessed 25 May 2023.

[43] Ibid.

[44] Brandon Vigliarolo, 'Microsoft HoloLens: Cheat Sheet' (*TECHREPUBLIC,* 30 July 2018) <https://tek.io/3bqSC9G> accessed 25 May 2023; Ash, 'Sorry Microsoft, Controllers Are a Must for AR Smart Glasses' (*Medium,* 13 September 2019) <https://bit.ly/2LrS5K1c> accessed 25 May 2023.

2.3. SOCIAL IMPLICATIONS OF IMMERSIVE TECHNOLOGY

As we have understood the mechanism of operation of Immersive Technologies it is now important for us to understand the social impacts on the users of immersive technology in order to figure out the challenges and gaps in terms of the functioning of Immersive Technology.

We have often seen that there is a tendency to perceive immersive media as a progression or enhancement of entertainment, interactive gaming, or internet-based social networking. The argument posits that the phenomenon is inherently distinct due to the coexistence of psychological and physiological components. It is imperative to initiate the process by understanding the similarities.[45] One forum that bears notable resemblance is social VR, owing to its deliberate emulation of conventional non-immersive social networking platforms. Nevertheless, it is important to note that this comparison might not be entirely applicable due to the emergence of gaming platforms such as Fortnite, which can blur the distinctions between online gaming, social media, and performance spaces. As an illustration, the musical artist Marshmello performed a concert in February 2019 within the virtual gaming platform Fortnite, attracting a staggering attendance of 10.7 million individuals from various global locations.[46] If the online live streaming of the performance were included in the tally, a greater number of individuals would have been accounted for as attendees. The official YouTube recounting was viewed by a total of over 27 million individuals.[47] Given the increasing fluidity of genres, attempting to define analogous media can be seen as a temporary endeavour, at most, aimed at enhancing our comprehension of the functioning of immersive media within a given society.

Comparable to social media and gaming platforms, diverse types of immersive media enable user engagement and communication with individuals situated at a distance. The facilitation of communication between entities is achieved through the utilization of interfaces that incorporate both hardware and software components. The utilization of digital platforms and immersive media has enabled individuals to establish connections with like-minded individuals, potentially across vast geographical distances, thus facilitating the formation of social groups. To date, the immersive industry has primarily focused on utilizing gaming as its principal means of dissemination. In 2016, the mobile game Pokémon Go garnered considerable attention by popularizing the notion of mobile AR among a broader demographic.

[45] Andrew Webster, 'Fortnite's Marshmello concert was the game's biggest event ever' (*The Verge,* 21 February 2019) <https://www.theverge.com/2019/2/21/18234980/fortnite-marshmelloconcert-viewer-numbers> accessed 25 May 2023.
[46] Ibid.
[47] Ibid.

The triumph of the game indicated that individuals were open to the notion of employing a mobile-based AR interface to identify and seize digital creatures in outdoor environments, and were prepared to actively pursue them.[48]

Oculus, a subsidiary of Facebook, has attained a noteworthy sales achievement by vending over 1.5 million VR headsets to end-users, which can be ascribed to the burgeoning prominence of gaming.[49] The Sony HTC Vive, a virtual reality system that competes in the market, has achieved a successful sales record of 1.3 million units.[50] HMDs that demonstrate exceptional performance have predominantly been geared towards entertainment-oriented programming, specifically interactive gaming experiences intended for end-users. The accomplishments suggest that VR technology, which is focused on consumer usage and supported by gaming applications, has achieved a noteworthy milestone. The adoption rates of AR and MR headsets have exhibited non-uniformity, potentially owing to the absence of a clearly defined use case for these technologies among average consumers, in contrast to enterprise or commercial customers.[51] AR technology has gained significant traction through the utilization of filters within popular image sharing and messaging applications, such as Snapchat filters. These entities are not conventionally perceived as AR, thereby illustrating the potential existence of this technology without users consciously acknowledging their transition to a novel medium.

Moreover, it would be inaccurate to give in to the temptation of considering immersive technologies as mere variations of already existing electronic interfaces and applying the same regulatory approaches to this emerging medium. The utilization of VR and AR technologies extends beyond their conventional employment in the domains of video games and social networks. This paper focuses on the challenges related to user safety and privacy that are frequently encountered in internet-based platforms. The incorporation of immersive technologies necessitates an examination of the psychological aspects that could potentially have noteworthy consequences for the basic human rights of the user.

[48] Susie Rack, 'How Pokémon Go has changed my life' (*BBC News*, 1 January 2020) <https://bbc.in/2WX6C5S> accessed 25 May 2023.
[49] Travis Hoium, 'Oculus Devices Sold Out in a Positive Sign for Virtual Reality' (*The Motley Fool*, 27 December 2019) <https://www.fool.com/investing/2019/12/27/oculus-devices-sold-out-in-positive-sign-for-virtu.aspx> accessed 26 May 2023.
[50] Ibid.
[51] A. J. Agrawal, '3 reasons augmented reality has not achieved widespread adoption' (*The Next Web*, 16 February 2018) <https://thenextweb.com/contributors/2018/02/16/3-reasons-augmented-reality-hasnt-achieved-widespread-adoption/> accessed 26 May 2023.

2.3.1. PSYCHOLOGICAL ATTRIBUTES ASSOCIATED WITH IMMERSIVE EXPERIENCES

Immersive technologies possess distinct attributes that differentiate them from other forms of innovation, such as social media. The primary factor is immersion, which refers to the user's perception of being present in an alternate environment.[52] To elucidate this concept for individuals who are not familiar with it, immersion creates an environment that establishes a particular context. Upon donning a headset and initiating the immersive encounter, such as within an aquatic marine setting,[53] The Blu offers users the opportunity to engage in an immersive virtual reality encounter with a humpback whale, resulting in a highly memorable and iconic experience. The user reviews of the products reflect a profound sense of immersion and wonder experienced by the users. One may observe that depictions of the ocean encompass the entirety of their visual field. The auditory emissions originating from marine organisms and gas bubbles seem to emanate from their anticipated physical positions, as if one were situated on the ocean floor.[54] The phenomenon of light transmission from the ocean surface to the bottom of the sea is observed in a downward direction. The user is exposed to various patterns of stimulation through the content, which may include light photons for visual perception, acoustic input for auditory perception, and tactile or haptic stimulators for the sense of touch. The presentation of these stimuli can induce a feeling of immersion in the user. In summary, the immersive characteristics of the programme result in a perception of authenticity between the user and the software by means of a comprehensive environment.

Furthermore, the technology encompasses distinct aspects of embodiment. It is imperative for users to possess a heightened sense of active presence.[55] The phenomenon under consideration has been characterized as "the illusion of non-mediation," whereby an individual experiences the perception of communicating without the presence of interfaces.[56] Jessica Outlaw, who serves as the director of the Outlaw Lab at Concordia University, conducts research on the impact of immersive technologies from a design perspective. The author provides a personal

---

[52] 'Hate in Social VR' (*Anti-Defamation League*, 7 December 2018) https://www.adl.org/resources/reports/hate-in-social-virtual-reality accessed 26 May 2023

[53] 'The Blu Franchise' (*Wevr*) <https://wevr.com/theblu> accessed 26 May 2023.

[54] 'Best VR Underwater Adventure Games for Deep-Sea Explorers' (*VRGAMECRITIC*) <https://vrgamecritic.com/article/best-vr-underwater-exploration-adventure-games> accessed 26 May 2023.

[55] J.N., Cummings & J.J., Bailenson, 'How immersive is enough? A meta-analysis of the effect of immersive technology on user presence' (2016) VHIL <https://vhil.stanford.edu/pubs/2016/how-immersive-is-enough/> accessed 26 May 2023.

[56] Eric Johnson, 'Full transcript: Stanford virtual reality expert Jeremy Bailenson on Too Embarrassed to Ask' (*VOX*, 4 August 2016) < https://www.vox.com/2016/8/4/12371450/jeremy-bailenson-stanford-university-virtual-reality-too-embarrassed-to-ask-podcast-transcript> accessed 26 May 2023.

anecdote to demonstrate how VR can facilitate genuine interpersonal interaction: "when while utilizing a VR headset, I engage in interpersonal communication with familiar individuals. This immersive technology provides me with a heightened sense of presence and embodiment, allowing for a more authentic experience. I generate recollections with individuals within these simulated environments."[57] The author perceives a negligible distinction between socializing with their acquaintances in a virtual environment versus interacting with them in person. Moreover, Jeremy Bailenson, a VR pioneer, and professor at Stanford University, highlights the importance of effectively implementing tracking, rendering, and display techniques to establish a sense of presence and prevent simulation sickness caused by cognitive disassociation among content creators.[58]

The third distinguishing factor between immersive experiences and social media networks is the notion of "embodiment," which refers to the sensation of perceiving one's virtual avatar or body as an extension of their physical self.[59] The phenomenon is aptly demonstrated through Mel Slater's "rubber hand illusion," wherein a simulated or physical toy hand is presented to a participant within their visual field, typically through a VR experiment. Individuals who viewed the experimentation conducted by researchers on the toy perceived the poking, prodding, and mistreatment as authentic physical encounters. The brain established a neural connection with the foreign entity.[60] The concept of embodiment has demonstrated potential benefits, particularly in clinical contexts where it has exhibited efficacy in mitigating phantom limb pain.[61] However, the proliferation of virtual social experiences also entails a significant potential hazard, given the prevalence of violence and harassment that have become synonymous with numerous online social platforms. Based on a study conducted by Pew Research, it has been found that 40% of individuals in the United States have reported experiencing personal online harassment.[62] Preliminary investigations conducted in the field

[57] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed on 26 May 2023.
[58] Jeremy Bailenson, *Experience on Demand: What Virtual Reality Is, How It Works, And What It Can Do* (1st edn, W.W. Norton & Company 2018) 17-20.
[59] Cortese, Michelle and Andrea Zeller, 'Designing Safer Social VR' (*Medium,* 2 November, 2019) <https://immerse.news/designing-safer-social-vr-76f99f0be82e> accessed 26 May 2023.
[60] Ibid.
[61] 'Virtual reality eases phantom limb pain' (*Sciencedaily,* 31 May 2017) <https://www.sciencedaily.com/releases/2017/05/170531102921.htm.> accessed 26 May 2023.
[62] Maeve Duggan, 'Online Harassment 2017' (Pew Research Center, 11 July 2017) <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/> accessed 26 May 2023.

of social virtual reality, such as those conducted by Dr. Outlaw, indicate a greater prevalence within this emerging platform.

So, the perception of being in an alternate reality is facilitated by the amalgamation of immersion, presence, and embodiment. In the realm of psychological research, it is frequently reported by users that they experience a sense of complete immersion in virtual experiences. The phenomenon of embodied experiences enables individuals to engage in complete interaction with the various aspects of their surroundings. In social or multi-user virtual environments, this interaction extends to other individuals present within the virtual space. The defining characteristic of these experiences extends beyond their immersive quality, encompassing the way our cognitive processes encode and retain perceptual information. According to Dr Thomas Furness, a pioneer in the field of immersive technologies, VRs possess a significant potential that can be likened to the immense power associated with splitting the atom. The reason for this phenomenon is attributed to the unparalleled ability of immersive experiences to stimulate spatial memory, surpassing that of any other medium.[63] This is further enhanced by the active nature of such experiences. The absence of a clear demarcation between the user and the objects of their interaction can prove advantageous in specific scenarios such as educational or therapeutic contexts. However, it can also pose challenges in virtual experiences that entail engaging in violent activities, as is the case with certain gaming applications. According to Furness, these experiences are indelibly imprinted on the brain, akin to being inscribed in permanent ink. Furness's claims are supported by findings in the field of neuroscience. The process by which our brains retrieve memories of virtual environments bears resemblance to the mechanisms underlying the formation of memories pertaining to real-life experiences. Upon conducting brain activity measurements through MRIs, researchers have observed that the response in the hippocampus when an individual recalls a virtual event is comparable to the response that would be expected in the case of an actual event.[64] The concept of psychological realness in immersive technologies elicits physiological responses from users that closely resemble their bodily reactions to actual situations.[65]

[63] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed on 26 May 2023.

[64] T.I. Brown et. al, 'Prospective Representation of Navigational Goals in the Human Hippocampus' (2016) 352 Science 1323.

[65] 'Understanding Sensors: Magnetometers, Accelerometers and Gyroscopes' (*Virtual Reality Society*, 2017), <https://www.vrs.org.uk/virtual-reality-gear/motion-tracking/sensors.html> accessed 26 May 2023.

According to Professor Mark Lemley, virtual reality and augmented reality can be described as a visceral experience. Phenomena that occur in virtual reality lack physical reality. For instance, in the Bullet Train game, the act of being shot by the antagonist does not result in actual death. However, they evoke a sense of realism. Subsequently, those emotions may result in tangible physiological effects. It is plausible that a game that induces a strong sense of realism could potentially cause a person to experience fear to the point of cardiac arrest. The immersive nature of VR technology allows individuals to undergo experiences that are not typically encountered through traditional mediums such as the Internet or non-VR video games, even if physical harm is not incurred.[66] So it can be understood that Immersive experiences are psychologically distinct from socializing in virtual game environments or engaging with others on social media platforms due to their multifaceted nature but due to a sense of realism it might have a physiological effect.

2.3.2. CONTENT-BASED CHARACTERISTICS OF IMMERSIVE INTERFACES

The faculties of sensory perception, along with their corresponding interfaces, represent additional dimensions of immersive technologies that afford users the ability to construct alternative realities. The production of effective immersive hardware necessitates two crucial components: those that facilitate measurement and those that enable the generation of stimuli.[67] Given that the technical aspects of immersive hardware have already been addressed, the focus will now be directed towards the crucial elements for constructing VRs.

Fundamentally, immersive technology is dependent on hardware to obtain signals. Initially, the method assesses distinct characteristics of physical motion and its operation, such as those pertaining to the cranium, the ocular organs, the upper limbs, the digits, and the lower extremities. Additionally, emotional, or physiological states can be assessed by means of electroencephalography or electromyography, which respectively involve the measurement and recording of electrical activity in various regions of the brain and the tracking of signals that stimulate muscles.[68]

Scholars have been contemplating the ramifications of collecting biometric data for a while. However, the researcher will expound upon in this paper, the incorporation of these methods

[66] 'Ubiquitous $90 billion AR to dominate focused $15 billion VR by 2022' (*Techcrunch*, 26 January 2018) <https://techcrunch.com/2018/01/25/ubiquitous-ar-to-dominate-focused-vr-by-2022/> accessed 26 May 2023.
[67] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed on 26 May 2023.
[68] Ibid.

into HMDs fundamentally alters the consequences of data gathering in immersive technology. The differentiation between personal information obtained through immersive technologies and personal information obtained through pure biometric data is primarily attributed to the amalgamation of bodily measurements with metrics pertaining to an individual's thoughts and emotions. This amalgamation holds significant importance in this regard and concerns of Privacy and Data Protection.

There exist various attributes of content that have the potential to augment the immersive characteristics of a virtual or augmented reality encounter. Initially, a comprehensive panoramic field of vision can induce a sense of immersion within the user, as if they are genuinely situated within an alternate environment. Achieving photorealistic image quality may not necessarily be essential. In fact, it has been observed that representative environments can often be more efficacious for users, as the brain is capable of filling in any missing details. It is imperative that the graphics are rendered at a satisfactory level of quality in order to evoke a sense of suspension of disbelief.[69]

As aforementioned, the implementation of 3D audio programming enables the simulation of sound originating from a specific direction and exhibiting changes in volume corresponding to the proximity of the listener to the source. This augmentation of auditory information enhances the user's perception of the virtual environment, rendering it more realistic.[70] Incorporating spatial mobility within an experience, facilitated by six degrees of freedom, can enhance the perception of reality in conjunction with auditory stimuli. The availability of cost-effective and highly mobile hardware such as the Oculus Quest and Oculus Go's untethered HMD has contributed to the creation of a heightened sense of presence in virtual environments, unencumbered by the constraints of mediation.[71] Recent advancements in touch-based technology, such as haptic gloves and hands-free controllers,[72] have the potential to enhance the realism of virtual reality experiences. Thus, such a setting concerns of human rights the immersive environments in terms of a combination of regulations governing content, data collection and use, behaviour, and actors, as well as technical system constraints.

[69] Ibid.
[70] Ibid.
[71] 'Hate in Social VR' (*Anti-Defamation League*, 7 December 2018) <https://www.adl.org/resources/reports/hate-in-social-virtual-reality> accessed 26 May 2023.
[72] Adi Robertson, 'Tesla suit's new VR gloves let you feel virtual objects and track your pulse' (*The Verge*, 27 December 2019) <https://bit.ly/2T2XcEv> accessed 26 May 2023.

2.4. NECESSITY OF IMPLEMENTING SAFETY MEASURES IN IMMERSIVE TECHNOLOGY

As we have discussed in the previous section about the social impacts of immersive technologies on its users and the concerns of human rights as a result of such impacts. Therefore, let us discuss the important question why do we need to implement safety measures in Immersive technologies? So that we can understand the safety which is required for the users of such Immersive Technologies.

Throughout history, the advent of novel forms of media, ranging from the telegraph to the telephone, from the television to the internet, has been accompanied by both the potential for advancement and a concomitant apprehension of risk. The immersive nature of VR and AR technologies, coupled with their psychological effects, have the potential to cause adverse impacts on individual users and their communities. Considering this, the researcher contend that it is imperative to scrutinise immersive media through a human rights-oriented perspective. The integration of human dignity into immersive systems through a human rights-based framework is comparable to the prioritisation of privacy-related concerns through privacy-by-design frameworks during the initial stages of product and policy development. From a human rights perspective, it is imperative for immersive creators and policymakers to scrutinise discrepancies between current privacy regulations and emerging forms of potential safety breaches that implicate the fundamental rights of users. Additionally, it is crucial to assess potential risks inherent in both the interfaces and the immersive content. In order to adopt a human rights-oriented perspective towards immersive technology, it is imperative to inquire about potential hazards that may arise from the integration of certain functionalities as customary attributes in conventional VR/AR equipment. What are the potential risks of user abuse or violations of the rights to freedom of expression, freedom of assembly, and user safety that can be reasonably foreseen? What are the characteristics of content moderation in an immersive setting? Is it necessary to reconsider the potential threats to privacy within immersive environments? Considering these inquiries, what measures can be implemented presently to safeguard human rights in digital domains? Exploring fundamental inquiries during the initial phases of immersive technologies' development could potentially prevent some of the challenges that have arisen in other internet-based technologies. Furthermore, this exploration could enable us to utilise this potent new medium in ways that are socially constructive and personally advantageous.

Furthermore, certain distinctive hurdles encountered by immersive media, encompassing issues pertaining to user safety and incongruity with prevailing biometrics regulations and the novel concept of biometric psychography as proposed by Brittan Heller in her paper 'Reimagining Reality' elucidates the distinctive nature of privacy-related risks in immersive technologies. This is attributed to the capacity of these technologies to establish a link between an individual's identity and their most intimate thoughts, preferences, and aspirations. Moreover, the author concludes this chapter by outlining potential advancements in the immersive industry and their potential impact on human rights, while also considering strategies for addressing any resulting challenges.

Now, when new media integrates the offline and online worlds, it presents significant challenges to both realms in terms of freedom of expression and public safety. And so moderating content poses a complex challenge for immersive technologies. The implementation of interventions through VR and AR technology can effectively mitigate specific user behaviours that manifest during immersive individual experiences. But, due to the dynamic and comprehensive qualities of immersive experiences, as well as the presence of active embodiment, threatening content such as violence can elicit a heightened sense of realism within virtual environments. This is since such content is not merely abstract, but rather extends beyond mere textual representation on a screen. The present paper will examine instances where safety-related violations of communal standards can potentially infringe upon users' entitlement to express themselves freely and assemble peacefully. This phenomenon bears resemblance to the way in which online harassment can stifle voices and compel marginalised individuals to withdraw from social media platforms.[73] In her work, Danielle Citron presents a similar viewpoint concerning the issue of online harassment within the realm of social media platforms. She asserts that such harassment has adverse effects on the rights of individuals to freely express themselves, as it seeks to stifle their voices.

Upon examining the various technical tiers involved in an immersive encounter, there exist diverse pathways for prospective content regulation. The scenario bears resemblance to the practise of content moderation on the internet, which entails a range of options and inquiries pertaining to power dynamics, actors involved, and accountability, contingent upon the various strata of the internet stack where moderation activities may transpire. The initial public discourse concerning the various layers of the internet stack and their influence on content

[73] Danielle Citron, 'Cyber Civil Rights' (2009) 89 Boston Univ. Law Rev.66 <https://ssrn.com/abstract=1271900> accessed 26 May 2023.

moderation emerged through the deliberation surrounding Cloudflare's decision to cease its provision of services to the notorious white supremacist website, the Daily Stormer.[74] The concept of the internet stack is employed to analyze the technical procedures involved in the establishment of online environments, encompassing various underlying network technologies and stakeholders responsible for the existence of websites.[75] Regarding immersive content, the initial level of moderation capacity would involve examining user conduct, as manifested through the behaviours and decisions exhibited by one's avatar within the virtual realm. The second aspect pertains to the substance of the simulated environment. The third factor pertains to the inherent features integrated within interfaces and platforms. Certain layers, such as the behaviour of avatars, may present a greater level of anticipated hazard compared to others. The issue of online harassment within virtual environments and digital communities has been extensively researched. It is possible to consider both the challenges and potential remedies that involve the various layers of user conduct, content, and platform functionality. Like social media, the targeting effects in VR disproportionately affect underrepresented demographics, specifically minority groups, women, and marginalised communities. The issue of online harassment within virtual environments and digital communities has been extensively studied. It is possible to envision both challenges and potential remedies that involve the various layers of user conduct, content, and platform functionality within these immersive systems. Like social media, the targeting effects in VR disproportionately affect underrepresented groups, specifically minorities, women, and marginalised communities.

Moreover, the term 'Social VR' pertains to digital platforms that facilitate interactive communication among users in virtual environments, allowing them to convene and engage in social activities within a shared digital space. Shortly after the emergence of social virtual reality, instances of user mistreatment within these environments began to surface. In 2016, Taylor Lorenz, a journalist, recounted her experience of accessing Altspace VR, a widely used VR platform for social interaction. She stated that:

> "Upon entering the welcome room, I received an uninvited "VR kiss" within a span of two minutes. Subsequently, my slender avatar with brown hair was inundated by male users who were rubbing against me and inquiring whether I was as slim or merely an overweight individual hiding behind an avatar. The experience

[74] Matthew Prince, 'WHY WE TERMINATED DAILY STORMER' (*Cloudflare,* 17 August 2017) <https://blog.cloudflare.com/why-we-terminated-daily-stormer/> accessed 26 May 2023.

[75] Henrik Frystyk, 'The Internet Protocol Stack' (*w3 org,* July 1994) <https://www.w3.org/People/Frystyk/thesis/TcpIp.html> accessed 26 May 2023.

> caused a sudden shift from the virtual realm to a reminiscent state of middle school."[76]

Her colleague, who likewise adopted a female avatar, encountered a comparable occurrence. Despite the implementation of moderators, terms of service prohibiting harassment and indecent conduct, and blocking mechanisms, Lorenz contends that the user demographics and social virtual reality functionality created a conducive environment for the misconduct.[77] In a recent expose on sexual harassment within virtual reality, a journalist who goes by the name Jordan Belamire shared a detailed account of her encounter with unwanted physical contact while participating in the VR archery game, QuiVr.[78] Belamire reported that her personal space was violated and her character was groped within a mere three minutes of gameplay. As per Belamire's testimony, the interaction unfolded in the following manner:

> "Amidst the onslaught of undead and malevolent entities that required our attention, I found myself in the company of BigBro442, anticipating our forthcoming assault. Abruptly, the helmet without a body belonging to BigBro442 was directed straight towards me. The individual's hand levitated towards my person and proceeded to engage in a virtual act of chest rubbing. I vocalised a command to cease the action. Belamire experienced a bout of laughter, potentially stemming from feelings of embarrassment and the absurdity of the circumstances. Women are often expected to maintain composure and tolerate instances of sexual harassment without expressing discomfort or objection. However, I advised him to discontinue his actions. The individual's provocation incited the subject's behaviour, persisting in pursuit even when the subject disengaged. The subject proceeded to engage in physical contact, simulating the act of grasping and pinching in the vicinity of the individual's chest. With a heightened sense of confidence, he proceeded to forcefully place his hand towards my digital pelvic region and initiated a rubbing motion. In the given scenario, the individual was subjected to virtual groping within a snowy fortress while being observed by their brother-in-law and spouse. As the interaction continued, my initially light-hearted remarks directed towards BigBro442 gradually escalated in intensity, becoming increasingly infused with exasperated profanity. Initially, my brother-in-law and spouse joined in with my amusement, as they were only able to perceive the 2D representation of the physical contact on the computer monitor. From an external perspective, the QuiVr world's complete immersion aside, the scene would have appeared amusing and lacking in authenticity. But just like the apparent verisimilitude of the one-hundred-foot fall. The sensation of virtual groping is perceived with a similar level of realism as physical groping. Even though undoubtedly, there is no physical contact involved, akin to the fact that one is not

[76] Taylor Lorenz, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here is Why I Keep Going Back' (*Mic*, 26 May 2016) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> 27 May 2023.
[77] Ibid.
[78] Jordan Belamire, 'My First Virtual Reality Groping' (*Medium*, 20 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 27 May 2023.

> truly elevated one hundred feet above the ground, nevertheless, the experience is still immensely frightening."[79]

Additional accounts of harassment within VR have been documented, with instances of targeting based on sexual orientation, gender, race, ethnicity, religion, and homophobia.[80] A study on the experiences of women in 'Social VR' was conducted by The Extended Mind, a research firm, in 2018. The outcomes were unsurprising given the experiences of Belamire and rather disheartening. Specifically, 49% of female participants reported encountering at least one instance of harassment while engaged in VR.[81] A significant proportion of individuals did not return to the virtual encounter. The incidence of harassment was not restricted to women alone, as revealed by the fact that 30% of male participants reported encountering racist or homophobic material, while 20% were subjected to comments or threats of a violent nature on the platform.[82]

Considering such apprehensions regarding user conduct, corporations have initiated the development of content moderation functionalities that consider user agency, intentionality, and authorization. Currently, several platforms have implemented a feature that creates a personal space buffer, which corresponds to offline cultural norms. This buffer typically spans approximately 12 to 18 inches around the user, providing a private area.[83] During the F8 conference, Oculus presented their approach to safeguarding the personal space of their users.[84] In the context of a Facebook social VR application, if one user's avatar encroaches upon another user's "safety bubble," both avatars will subsequently become imperceptible to each other. However, at that time these were Facebook Spaces and Oculus Venues. These were shut down on October 25, 2019 as Facebook Oculus prepared to launch Facebook Horizon, its new social VR platform in which such safety bubbles around avatars were made into operation.[85] Additional configurations afford the user with the capacity to withdraw their consent to engage

[79] Ibid.
[80] 'Hate in Social VR' (*Anti-Defamation League*, 7 December 2018) <https://www.adl.org/resources/reports/hate-in-social-virtual-reality> accessed 27 May 2023.
[81] Jessica Outlaw, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users' (*Medium*, 4 April 2018) <https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers> accessed 27 May 2023.
[82] Ibid.
[83] James J. Cummings and Jeremy N. Bailenson, 'How immersive is enough? A meta-analysis of the effect of immersive technology on user presence' (2016) VHIL <https://vhil.stanford.edu/pubs/2016/how-immersive-is-enough/> accessed 27 May 2023.
[84] Michelle Cortese and Andrea Zeller, Designing Safer Social VR, (*Medium,* 2 November 2019) <https://immerse.news/designing-safer-social-vr76f99f0be82e> accessed 27 May 2023.
[85] Sam Tabahriti, 'Meta is putting a stop to virtual groping in its metaverse by creating 4-foot safety bubbles around avatars' (*Business Insider India*, 5 February 2022) <https://www.businessinsider.in/tech/news/meta-is-putting-a-stop-to-virtual-groping-in-its-metaverse-by-creating-4-foot-safety-bubbles-around-avatars/articleshow/89367619.cms> accessed 27 May 2023.

in social activities. The option to "Pause" enables a user to discontinue the activity within a VR environment in the event of discomfort. It is possible for a user to utilise the 'mute' function to render another user's avatar completely invisible. The applications are equipped with real-time moderators who assist in monitoring and regulating inappropriate conduct.[86] The prompt response of the QuiVr developers to the reported incidents of groping is noteworthy. They implemented corrective measures in a timely manner, surpassing the actions taken by Oculus. A personal space bubble was devised to encompass an entire individual, in contrast to Oculus which only targeted specific body parts.[87] Moreover, there has been a notable level of responsiveness among individual developers with regards to addressing certain concerns pertaining to user safety. Harmonix, a developer partner of Facebook, manages a multi-player lounge within their Dance Central VR experience. If an individual perceives an encroachment upon their personal space, they may opt to utilise a hand gesture consisting of two thumbs pointed downward towards the avatar of the individual engaging in harassing behaviour. The individual engaging in harassing behaviour is subjected to a muting and freezing protocol, followed by a relocation to a different section of the dance floor.[88]

As immersive spaces continue to develop into interactive communities beyond conventional 'Social VR' platforms, the significance of prevention measures will become more pronounced. As previously stated, certain novel platforms will encompass the spatial computing spectrum, encompassing VR, as well as conventional computer and smartphone technologies such as Mozilla MR. Mozilla's Hubs is a social platform that facilitates collaboration in virtual reality or via a "flat" screen on desktop or mobile devices through the utilisation of spatialized audio, 3D environments, and media composition features. In the context of mixed spaces, it is imperative to consider the potential psychological effects of immersive media. Additionally, it is crucial to prioritise measures that prevent user abuse and unwanted contact.

As immersive technology continues to advance, prioritising prevention measures is imperative. In September of 2019, Oculus made public the introduction of Facebook Horizon, an upcoming virtual reality-based social environment designed for use with the Oculus Quest and Rift

[86] Mark Sullivan, 'Virtually violated: How Facebook is trying to fix abuse on social VR before it goes mainstream' (*Fast Company*, 5 February 2019) <https://www.fastcompany.com/90342844/abuseon-social-vr-facebook-is-trying-to-fix-it-before-it-goes-mainstream> accessed 27 May 2023.
[87] Mark Lemley and Eugene Volokh, 'Law, Virtual Reality, and Augmented Reality' (2018) 166 U. PA. L. REV., 87-88.
[88] Mark Sullivan, 'Virtually violated: How Facebook is trying to fix abuse on social VR before it goes mainstream' (*Fast Company*, 5 February 2019) <https://www.fastcompany.com/90342844/abuseon-social-vr-facebook-is-trying-to-fix-it-before-it-goes-mainstream> accessed 28 May 2023.

Platforms, revealed in the year 2020.[89] The organisation expounds on the operational mechanics of the new platform, which is designed to function as a comprehensive virtual realm. The Horizon experience commences with a lively town square that serves as a hub for social interaction. Subsequently, it extends into an interlinked realm that enables individuals to discover new locations, engage in gaming activities, establish communities, and even generate original experiences. Prior to entering Horizon for the initial time, individuals will engage in the creation of their own avatars, utilising a diverse range of style and body options, thereby facilitating the complete expression of their unique identities. Subsequently, individuals will be transported through tele pods, which resemble magical portals, from communal areas to uncharted territories brimming with opportunities for adventure and discovery. Initially, individuals will engage in games and immersive encounters developed by Facebook, such as Wing Strikers, a collaborative airborne encounter. However, this is merely the initial phase. Individuals may also engage with a multitude of additional Horizon realms, which are constructed utilising the World Builder. This is a set of user-friendly creation instruments. Individuals will possess the ability to construct novel environments and engagements, ranging from warm, leisurely locations to dynamic, participatory spaces, without any prior knowledge of programming. Thus, the Facebook Horizon will facilitate a hospitable atmosphere for individuals who opt to construct, engage in recreational activities, or socialise by implementing novel safety mechanisms and human advisors, known as Horizon Locals, who will be available to address inquiries and offer support, if necessary.[90]

This will hold greater significance particularly in completely immersive digital environments such as Horizon. The QuiVr example demonstrates that virtual spaces can elicit perceived threats, such as encroachment on physical space, user intimidation, or even avatar assault, which may be processed by the human brain as genuine threats. Individuals might have trouble in distinguishing between the emotional responses elicited by virtual and physical assault due to cognitive factors. The latest advancements of Horizon are being incrementally implemented, with additional updates having been disseminated in December of 2019. The features encompassed communication with acquaintances on Oculus, as well as the exchange of visual media such as photos and videos, and the ability to broadcast live content to the Facebook platform. It is possible to generate events to schedule gaming sessions with acquaintances or

[89] Meta Quest Blog, 'Introducing 'Facebook Horizon,' a New Social VR World, Coming to Oculus Quest and the Rift Platform in 2020' (*Meta,* 25 September 2019) < https://www.meta.com/blog/quest/introducing-facebook-horizon-a-new-social-vr-world-coming-to-oculus-quest-and-the-rift-platform-in-2020/> accessed 28 May 2023.
[90] Ibid.

coordinate gatherings, and establish groups that are open for participation by all Oculus associates of the groups. When links are shared via Messenger, it is possible for Facebook friends to form groups with the user in VR.[91] In order to access the features, users will be prompted to authenticate their identity on Facebook. Additionally, users will be encouraged to engage in social activities such as attending events, expanding their social network, and exploring other users' profiles.[92] Although it is not a compulsory requirement to log in, the Facebook data provided by users will be utilised for the purpose of social functionalities, recommendations, targeted advertising, and virtual reality events and promotions. The level of integration between Oculus and Facebook services is expected to increase, as new functionalities, including Facebook Group sharing options and watch parties on Quest, are anticipated to be introduced.[93] Should the initial obstacles of 'Social VR' remain unresolved, it is probable that they will be amplified and transformed into fresh predicaments within innovative settings such as Hubs and Horizon. In these environments, user-generated content will introduce new prospects for creativity and self-expression, but also for exploitation and mistreatment.

Furthermore, with the increasing involvement of prominent corporations such as Mozilla and Facebook in the realm of immersive technology, the growing interconnection between social media platforms and social VR platforms could potentially raise concerns among proponents of safeguarding user privacy.[94] Facebook has made efforts to address these concerns. As stated in the frequently asked questions (FAQ) section, it is not necessary to authenticate with Facebook in order to utilize the VR platform. By doing so, users will retain their current Oculus friends, username, and profile. Users have the option to choose whether to publicly disclose their actual name, as it appears on their Facebook profile, on the Oculus platform. Additionally, they can decide whether to automatically include their Facebook friends as contacts on Oculus. Users will possess the ability to exercise control over the content they choose to share from Oculus to Facebook, as well as determine the audience that can access and view said posts. The modifications to the privacy policy will have no impact on third-party applications and games.

[91] Ibid.
[92] Ibid.
[93] Meta Quest Blog, 'Introducing New Features from Facebook to Help People Connect in VR and an Update to Our Privacy Policy' (*Meta*, 11 December 2019) < https://www.meta.com/blog/quest/introducing-new-features-from-facebook-to-help-people-connect-in-vr-and-an-update-to-our-privacy-policy/> accessed 28 May 2023.
[94] Ibid.

The FAQ document provides a comprehensive delineation of the specific categories of data that will be shared between Oculus and Facebook in the event of account connection.

2.5. CHALLENGES IN IMMERSIVE TECHNOLOGY

The implementation of AR/VR technology exhibits potential in advancing inclusiveness and fairness in both digital and non-digital realm. To achieve the goal, it is crucial for leaders in the industry and policymakers to implement measures aimed at mitigating any unintended consequences.

The utilisation of AR/VR immersive technologies has the potential to transform the way individuals participate in work, education, and social interaction by enabling them to experience digitally generated content in both physical and virtual settings. The facilitation of global collaboration among workers can potentially improve economic opportunities by mitigating the challenges posed by geographical barriers. Furthermore, this has the potential to improve the accessibility of crucial services such as healthcare and education, while also creating innovative opportunities for social engagement. In addition, their adeptness in manipulating elements of digital environments, whether in part or in whole, allows them to proficiently address a diverse array of user needs, including accessibility features and privacy preferences. Immersive technologies possess the capability to enhance the inclusivity and equity of both digital and non-digital services and environments.

Nevertheless, there exist significant challenges that demand the attention of both corporate executives and government officials to augment the availability of immersive technologies across diverse populations and to proactively address any unanticipated ramifications. It is crucial for individuals to consider a multitude of factors, including but not limited to privacy, health, and safety risks, which may have adverse effects on both users and non-users of AR/VR technologies. Furthermore, it is imperative to consider the financial, physical, technical, and societal barriers that diverse user demographics may face when endeavouring to embrace or employ AR/VR technologies and software. The presence of bias and discrimination presents a noteworthy hazard in crucial areas such as employment, education, and government services. Considering these considerations can prove advantageous for numerous users as it can mitigate the likelihood of malevolent exploitation of the technology or any inadvertent outcomes that may hinder the advancement of AR/VR adoption. It is expected that employers, educators, and government agencies will require resolution of various challenges prior to the widespread adoption of AR/VR technologies. In order to tackle these obstacles, it is imperative for

technology designers and implementers to comprehend the viewpoints and real-life encounters of a wide-ranging group of individuals. To ensure that AR/VR technology promotes inclusivity and equity, it is imperative to consider the perspectives of vulnerable, marginalised, and underserved individuals and communities who have been historically underrepresented in policy and product development discussions. This encompasses a wide range of groups, such as communities of colour, individuals with disabilities, the LGBTQ community, survivors of abuse, socially or physically isolated individuals, children, older adults, low-income individuals, and other groups that are already at an increased risk of experiencing harm and exclusion in the physical world.

Significant endeavours are currently in progress within the industrial and policy spheres to contemplate potential mitigation strategies and proactively establish and execute AR/VR solutions that cater to the requirements of a diverse spectrum of users. The present paper in this chapter will elucidate several key factors that ought to be considered by developers, policymakers, and implementing organisations in their endeavours. This study delves into the apprehensions that equity and inclusion advocates prioritise in relation to AR/VR technologies, based on insights gathered from interviews with stakeholders who possess both expertise and personal experiences with these challenges. Subsequently, the chapter will delve into the ramifications of said risks and challenges on the innovation and adoption of AR/VR technology in various industries.

2.5.1 DISCUSSION ON RISKS AND CHALLENGES DEALT WITH BY VULNERABLE USERS IN AR/VR

The potential of AR/VR for entertainment, productivity, education, and communication is being increasingly recognised by individuals and organisations across various sectors. The user population is consistently increasing. According to a projection, approximately 18% of the populace in the US engaged with VR while 28% utilised AR at a minimum of one instance per month in the year 2021.[95] Notwithstanding the advancements in technology, there exist obstacles that may impede or dissuade a considerable proportion of users and wider communities, who are predominantly individuals that have been marginalised and underserved, from accessing and making complete use of these technologies. The aforementioned factors encompass amplified concerns regarding privacy, health, and safety, as well as obstacles to the

[95] Victoria Petrock, 'US Virtual and Augmented Reality Users 2021' (*Insider Intelligence,* 15 April 2021) <https://wwwemarketer.com/content/us-virtual-augmented-reality-users-2021> accessed 28 May 2023.

accessibility and integration of immersive experiences. Additionally, there is a possibility for the exacerbation of prejudice and unfair treatment in both virtual and tangible environments. Individuals and communities who encounter increased vulnerability to personal safety and autonomy daily due to factors such as age, race, gender, sexuality, disability, or other aspects of their identity are likely to exhibit heightened sensitivity towards these issues. Minority communities are susceptible to experiencing prejudice, unfair treatment, and intimidation due to their racial or religious background. Consequently, they may be more exposed to negative consequences resulting from breaches of their privacy that expose confidential or potentially identifiable data that they did not intentionally reveal.

By proactively identifying these obstacles, developers and organisations can construct and execute AR/VR solutions that are more efficient, and circumvent any unfavourable consequences or limitations that could have been readily averted. Given the novelty of these technologies, developers could draw from the shortcomings of previous digital communication technologies and design products that prioritise user safety, accessibility, and other pertinent factors.

2.5.1.1 RISKS & CHALLENGES ASSOCIATED WITH PRIVACY, HEALTH, AND SAFETY FOR VULNERABLE USERS WITHIN AR/VR

To promote inclusivity and maximize the benefits of immersive experiences for diverse individuals and communities, it is crucial for AR/VR devices and applications to consider the distinct needs of various user groups to foster a sense of comfort and security. The ramifications of extensive data gathering, the subjective feeling of complete immersion in both positive and negative virtual experiences, and the physical requirements of AR/VR equipment may lead to certain user privacy, health, and safety requirements being disregarded in the absence of protective measures. It is strongly advised that developers give precedence to the development of immersive experiences that fully consider the requirements of their most susceptible users and communities. The execution of this measure will establish a sturdy basis for guaranteeing confidentiality, well-being, and security within the framework of AR/VR solutions.

In addition, it is crucial to note that certain communities that are susceptible to harm and discrimination may face potential risks when revealing aspects of their identity. Therefore, having agency over the timing, manner, and audience of such disclosures is of utmost significance. The employment of AR/VR technologies entails distinct and amplified privacy hazards, owing to the extensive, comprehensive, and delicate nature of the data that these

innovations necessitate for their functioning.[96] It is noteworthy that these risks have implications that go beyond the users of the device. AR technologies and their associated applications have the potential to capture information about non-users or private spaces during the processing of audio, visual, or spatial data related to a user's environment. Additionally, these technologies may provide users with real-time, potentially aggregated information that could potentially disclose private details about other individuals. In the absence of protective measures, malevolent entities may exploit these technologies to engage in stalking, harassment, and other forms of infringement upon the privacy and self-governance of individuals.[97] The integration of audiovisual recordings with other identifiable data by AR devices and applications may pose a significant threat to vulnerable individuals, including abuse survivors or those who prefer to remain anonymous in certain environments.[98] Hence, individuals involved in the creation and execution of AR solutions for public or consumer use must contemplate feasible transparency measures to safeguard the privacy of onlookers. At present, the predominant method involves utilizing a visual indicator, such as an LED light, to apprise onlookers of a device's recording status. However, as these devices continue to advance, there exists substantial potential for developers to investigate more inventive means of promoting transparency and user agency.[99]

The continuous recording and processing functionalities of AR devices, coupled with the substantial quantities of possibly identifiable data amassed during VR encounters, may have significant implications for civil liberties. The utilization of AR devices by law enforcement to collect and consolidate real-time data may pose a potential threat to the First and Fourth Amendment rights as provided in the Constitution of US, particularly in communities that are already subjected to disproportionate targeting by law enforcement.[100] Similar threat is also applicable to other democratic nations too. Likewise, information obtained from a VR device

[96] Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 28 May 2023.

[97] Mary Anne Franks, 'The Desert of the Unreal: Inequality in Virtual and Augmented Reality' (2017) 51 UC Davis Law Review <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Franks.pdf> accessed 28 May 2023.

[98] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 28 May 2023.

[99] Ellysse Dick, 'How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces' (*Information Technology and Innovation Foundation,* 14 December 2021) <https://itif.org/person/ellysse-dick.> accessed 28 May 2023.

[100] Mary Anne Franks, 'The Desert of the Unreal: Inequality in Virtual and Augmented Reality' (2017) 51 UC Davis Law Review <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Franks.pdf> accessed 28 May 2023.

or application has the potential to disclose a substantial quantity of personal data about an individual if disseminated. Further measures are required to ensure the protection of Fourth Amendment rights provided under US constitution in relation to the access of real-time information and user data by government and law enforcement agencies.[101]

AR/VR technologies possess a variety of multimodal data collection capabilities, such as motion and eye tracking, location, and spatial mapping, and user-provided biographical or identifying data. These data collection methods frequently exhibit a strong correlation with personal information that individuals may wish to keep confidential. AR/VR devices and applications can utilize biometric inputs, such as gaze or movement, to deduce information pertaining to characteristics such as race, gender, age, or disability. This may potentially impede individuals' agency in deciding the timing, manner, and audience for disclosing various facets of their identity.[102] According to Cynthia Bennett, a researcher at the Human-Computer Interaction lab at Carnegie Mellon University, the potential use of personal identity information against individuals raises significant concerns that require careful consideration when addressing user privacy.[103] In the event that an employer were to incorporate a VR simulation into their recruitment procedures, the information obtained during a given session may potentially disclose a candidate's disability status. This could potentially result in unconscious prejudice or discriminatory hiring practices being directed towards said candidate. The act of involuntary disclosure, as described, can potentially infringe upon the candidate's personal autonomy and ability to control the information they choose to disclose to prospective employers, despite the legal protections afforded by anti-discrimination laws both nationally and internationally. The implementation of user privacy measures, such as limiting third-party access to personal data, can effectively reduce the likelihood of inadvertent discrimination or malevolent exploitation of sensitive information associated with these technologies.

Furthermore, the issue of harassment and abuse is a prevalent concern across various communication technologies, ranging from social media platforms to private messaging services. The hazards are not exclusive to VR technology, nor are they limited to digital media.

---

[101] Ellysse Dick, 'How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces' (*Information Technology and Innovation Foundation,* 14 December 2021) <https://itif.org/person/ellysse-dick.> accessed 28 May 2023.

[102] Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 28 May 2023.

[103] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 28 May 2023.

They are particularly pertinent to individuals who are already susceptible and underprivileged, such as women, persons with disabilities, ethnic minorities, and members of the LGBTQ community. Numerous platforms and communication tools have encountered difficulties with the inadvertent outcomes of their services on the psychological and emotional welfare of users who undergo harassment and abuse. The versatile characteristics of AR/VR technology, such as its ability to support multi-user interactions, offer the possibility for developers and implementing organizations to proactively establish effective protective measures against potential misuse. However, this requires a thorough comprehension of the technology's potential vulnerabilities.

It is crucial to comprehend that the safety considerations of users hold significant importance in the realm of VR owing to the heightened sense of presence and embodiment that immersive experiences provide to the user. Research has demonstrated that individuals perceive their avatars, which are digital depictions of themselves in VR, as an extension of their own identity.[104] Regrettably, the capacity of VR to simulate the physical realm in a digital environment also entails the potential for accurately and persuasively emulating physical maltreatment. The observation can be made that immersive spaces are not only susceptible to verbal harassment but also to physical abuse and sexual harassment.[105] The various types of harassment and abuse can result in significant psychological consequences, especially for those who have encountered or are highly susceptible to comparable behaviours in their tangible surroundings.

According to Carlos Gutierrez, the deputy director of the nonprofit organization LGBT Technology Partnership and Institute, the content present in this environment may potentially trigger individuals who have experienced similar forms of abuse.[106] Numerous users of social VR have encountered instances of harassment.

Moreover, according to a survey conducted on 600 social VR users, a significant proportion of both male and female respondents, specifically over one-third of males and nearly half of

[104] Philippe Bertrand et al, 'Learning Empathy through Virtual Reality: Multiple Strategies for Training Empathy-Related Abilities Using Body Ownership Illusions in Embodied Virtual Reality' (*Front Robot AI*, 2018) <https://www.frontiersin.org/articles/10.3389/frobt.2018.00026/full> accessed 28 May 2023.
[105] Jessica Outlaw, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality Users' (*Virtual Reality Pop*, 4 April 2018) <https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers.> accessed 28 May 2023.
[106] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation*, 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 28 May 2023.

females, reported instances of sexual harassment in VR.[107] The participants in the study conveyed instances of both verbal and physical forms of harassment directed towards their virtual representations, with the intention of discriminating against their gender, race, or sexual orientation.[108]

In a separate investigation involving female individuals who were novices in the realm of social VR, a considerable number of the subjects exhibited cognizance of sexism and gender-oriented mistreatment within the virtual environment and adopted protective or anticipatory measures, such as evading sizable groups or refraining from interacting with unfamiliar individuals.[109] As per the statement made by a participant, it was noted that there exist certain real-world experiences which they do not wish to undergo virtually.[110]

However, the VR platforms have the potential to mitigate certain hazards. In social VR environments, established protocols such as safety bubbles, which are imperceptible boundaries surrounding an avatar that restrict other avatars from encroaching on a user's personal space in a virtual setting, and other safety measures have become customary.[111] Similarly, specific VR applications, particularly those that provide social VR experiences, will be required to establish their own user safety protocols and implementation mechanisms, akin to the approach adopted by other online platforms in dealing with harassment and mistreatment at present. As an illustration, a social media platform may prohibit a user who participates in misconduct.

Ultimately, if multi-user VR applications are adopted by employers or institutions such as educational establishments, it will be incumbent upon them to address any instances of inappropriate conduct that may arise within the virtual realm. An instance of a business utilizing AR/VR devices for collaborative purposes could potentially implement regulations that impose disciplinary actions for any misconduct exhibited within virtual workspaces. Developers and implementing organizations can enhance user protection by establishing unambiguous and suitable accountability mechanisms for virtual harassment and abuse across

---

[107] Jessica Outlaw, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality Users' (*Virtual Reality Pop*, 4 April 2018) <https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers.> accessed 28 May 2023.
[108] Ibid.
[109] Jessica Outlaw and Beth Duckles, 'Why Women Don't Like Virtual Reality: A Study of Safety, Useability, and Self-Expression in Social VR' (*The Extended Mind*, 16 October 2017) <https://static1.squarespace.com/static/60e8ceb4ae52881d57698bf6/t/6164b95156a52d3614c29e82/1633990999726/The-Extended-Mind_Why-Women-Don%27t-Like-Social-VR_2017.pdf> accessed 29 May 2023.
[110] Ibid.
[111] Ibid.

various contexts. In addition, it is imperative for platforms and implementing organizations to solicit feedback from individuals who are frequently subjected to online harassment and abuse, as they contemplate the integration of safety protocols in VR applications.[112] Platforms with good intentions may unintentionally cause harm to their intended beneficiaries if they are designed without soliciting input from said beneficiaries. This phenomenon has already been observed in digital media that exists in 2D. In 2019, TikTok implemented measures to mitigate online bullying by restricting the visibility of videos produced by specific users, including individuals with physical or cognitive impairments. The policy in question was subject to criticism by disability advocates who contended that it was formulated without adequate consultation and curtailed the autonomy of creators in determining their own safety.[113] Improved engagement during the initial stages can serve as a preventive measure against such errors.

Moreover, despite being virtual, immersive experiences can exert palpable effects on an individual's physical reality. It is imperative for AR/VR devices and applications to account for the potential health and safety ramifications that may arise for a wide range of users, particularly those who are most susceptible to adverse effects. The integration of virtual elements into the physical world, whether through merging or complete replacement, can have an impact on situational and spatial awareness. This alteration may lead to an increased risk of accidents due to distractions or sensory obstructions. This holds true for all users; however, the peril is most pronounced for individuals who depend on assistive technologies to attain a perception of their environment that may be overlooked by others. In the context of VR, it is common for users to depend on auditory cues to sustain a degree of spatial awareness despite being fully engrossed in the VR experience. However, individuals who are deaf or have hearing impairments are unable to utilize this sensory modality to establish a connection with their physical environment. This places them at a heightened risk in the event of an emergency signal, such as the activation of a smoke alarm.

Attempts to tackle such concerns frequently yield additional advantages, such as safeguarding the well-being of individuals who utilize noise-cancelling headphones and possess the ability

[112] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[113] Adi Robertson, 'TikTok Prevented Disabled Users' Videos from Showing Up in Feeds' (*The Verge,* 2 December 2019) <https://www.theverge.com/2019/12/2/20991843/tiktok-bytedance-platform-disabled-autism-lgbt-fat-user-algorithm-reach-limit.> accessed 29 May 2023.

to hear. Numerous VR devices are equipped with safety mechanisms that expeditiously redirect users to their tangible surroundings. These features may comprise of external cameras that exhibit the physical environment when users transgress predetermined boundaries, or the capacity to exhibit virtual replicas of furniture within an immersive setting. Enhancing features aimed at enhancing user' situational awareness would effectively reduce safety hazards in both personal and professional contexts. The implementation of AR/VR technologies may result in adverse physiological reactions, which can pose a risk to the user's well-being. Developers must prioritize the mitigation of these effects to maximize the potential user base of their devices and applications. The effects frequently have a negative impact on individuals who are not adequately represented in the product development process or within a prospective user population. A frequently cited illustration of this phenomenon is the varying degrees of vulnerability among users to "cybersickness," which refers to a feeling of motion sickness experienced within a virtual setting. According to a study, it was hypothesized that females were more prone to encountering this phenomenon due to encountering more challenges in adapting the display to their visual needs.[114] The suitability of a device's fit can have a significant impact on the comfort and usability of AR/VR devices across a diverse spectrum of users. Individuals who utilize glasses or other head-worn assistive devices, such as cochlear implants, may encounter challenges when attempting to calibrate a HMD to their specific requirements.[115] During a study conducted in Nairobi, a researcher observed that VR headsets were ill-fitting for several participants who had thick braids or head coverings.[116] The level of comfort experienced by users of wearable AR/VR devices or controllers may not solely depend on the fit of the device, but also on the degree of contact with it. For instance, individuals who exhibit hypersensitivity to touch or textures may encounter difficulties in using such devices or controllers, especially over an extended period. Involving a diverse set of prospective users in the initial stages of product development can prevent the need for significant post hoc modifications by developers.

[114] Kay Stanney et al., 'Virtual Reality is Sexist: But It Does Not Have to Be' (*Frontiers in Robotics and AI,* 31 January 2020) < https://www.frontiersin.org/articles/10.3389/frobt.2020.00004/full> accessed 29 May 2023.
[115] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[116] Arwa Michelle Mboya, 'The Oculus Go Wasn't Designed for Black Hair' (*Debugger*, 5 November 2020) <https://debugger.medium.com/the-oculus-go-a-hard-ware-problem-for-black-women-225d9b48d098.> accessed 29 May 2023.

2.5.1.2. RISKS AND CHALLENGES OF ACCESS AND INCLUSION FOR VULNERABLE USERS IN AR/VR

Addressing the complex and often interrelated barriers to access that could impede the progress and adoption of AR/VR technology is imperative for both industry leaders and policymakers. The technologies that hold the greatest promise for benefiting specific communities are often impeded by inequitable barriers that hinder their accessibility or utilization. Lydia X.Z. Brown, who holds the position of general counsel at the Centre for Democracy and Technology and is an advocate for disability rights, issued a warning that immersive experiences possess the capacity to enhance accessibility to specific opportunities and areas, while also intensifying and exacerbating pre-existing inequalities and inaccessibility.[117] It is advisable for AR/VR device and application developers and implementers, with the aim of catering to diverse sectors, to embrace a comprehensive approach towards accessibility and inclusivity. The proposed approach ought to consider the plausible physical, technical, and non-technical hindrances, alongside the intersectional aspects that could hinder the acceptance and implementation of the solution.

In addition, Cynthia Bennett, a researcher from Carnegie Mellon University, has observed that the development of technology often prioritizes innovation over accessibility, with accessibility being considered only as a secondary concern.[118] This approach frequently leads to the implementation of expensive and improvised measures to ensure compliance with basic accessibility standards and to accommodate the requirements of users with disabilities. There is a growing apprehension among disability advocates regarding the perpetuation of this pattern in the realm of AR/VR. Immersive experiences pose intricate accessibility challenges for individuals with mobility, vision, hearing, speech, and cognitive impairments due to their inherently multisensory nature.[119] The technologies pose a considerable challenge, and in some cases, an insurmountable obstacle, for individuals with disabilities as well as those who experience temporary limitations in sensory or motor functions. An instance of a user's situation could entail being in a seated position, carrying a load with their upper limbs, or operating the device amidst a cacophonous environment. It is unlikely that most users,

[117] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[118] Ibid.
[119] 'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (*XR Association*, October 2020) <https://xra.org/wp-content/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 29 May 2023.

irrespective of their proficiency, would be able to consistently recreate the ideal setting for an optimal experience.

Consequently, a multitude of fundamental accessibility factors can enhance the general usability of numerous AR/VR solutions. Primarily, it is imperative that AR/VR devices are made accessible. The ability to configure and operate the apparatus that facilitates immersive encounters is imperative for users, spanning from handheld devices such as smartphones to wearable gadgets like smart glasses, as well as input devices like controllers and head-mounted displays. According to Larry Goldberg, a prominent member of the XR Access Initiative, ensuring accessibility of hardware and underlying platforms is a crucial aspect of achieving overall accessibility.[120] Failure to do so may result in inaccessible applications despite their accessibility features. Presently, several consumer devices available in the market do not fulfil the fundamental accessibility requirements of disabled users.[121] The devices' platforms, applications, and immersive experiences entail distinct accessibility considerations.[122]

Primarily, a considerable number of AR/VR applications necessitate a certain degree of physical movement, thereby rendering it arduous or unfeasible for persons with restricted mobility to execute actions essential for manoeuvring or engaging with virtual components. The utilization of audio-visual components to create virtual spaces can pose challenges for individuals who are deaf, hard of hearing, blind, low-vision, or deaf-blind, as these immersive experiences may not provide sufficient alternatives to accommodate their needs. Lastly, individuals who are susceptible to cognitive or sensory overload, such as those with cognitive disabilities or photosensitive epilepsy, may encounter challenges or hazards when attempting to navigate fully immersive experiences or substantially augmented physical environments.[123] Thankfully, it is feasible to cater to a significant number of accessibility requirements as an integral component of the overall user experience of AR/VR devices and applications, rather than as an add-on. In essence, the degree of customization that users can achieve in their virtual environments is the determining factor. Other digital platforms have already incorporated

[120] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[121] Kaitlin Ugolik Phillips, 'Virtual Reality Has an Accessibility Problem' (*Scientific American,* January 29 2020) <https://blogs.scientificamerican.com/voices/virtual-reality-has-an-accessibility-problem> accessed 29 May 2023.
[122] 'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (*XR Association,* October 2020) <https://xra.org/wpcontent/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 29 May 2023.
[123] Alice Wong et al, 'VR Accessibility Survey for People with Disabilities' (*Disability Visibility Project*) <https://www.ben-peck.com/papers/VR_Accessibility_Survey.pdf> accessed 29 May 2023.

accessible user preferences, such as automated captioning for video calls and default text enlargement on mobile devices. In the realm of VR, certain enthusiasts with disabilities have devised software-based and low-tech "hacks" to facilitate their use of such devices and enable their participation in VR experiences.

According to a survey conducted on individuals with disabilities who use VR, a significant number of them depended on adaptations such as the customization of open-source code, repositioning themselves within the play area to approach virtual menus or other objects, or supplementing device controls with more accessible hardware.[124] It is improbable and impractical to anticipate that individuals who use technology casually would opt for or possess the capability to allocate the essential time and resources to customize these technologies to suit their requirements. It is imperative for developers to prioritize accessibility for a diverse range of users in terms of both inputs (i.e. the means by which users control and interact with virtual elements) and outputs (i.e. the manner in which the virtual environment is presented to users) during the development of AR/VR solutions.[125] The absence of a clearly defined standard for accessible design of devices or applications highlights the pressing need for the establishment of best practices in the development of AR/VR technologies that are accessible. While web accessibility guidelines may provide guidance for certain aspects, they were originally developed for digital media that is 2D and are insufficient for immersive 3D.[126] During a roundtable discussion held on April 20, 2021, various stakeholders involved in disability rights and accessible design expressed their apprehension regarding this matter. While there are ongoing efforts to revise web accessibility guidelines to accommodate immersive experiences, it is important to note that several factors related to AR and VR cannot be simply transferred or modified from existing 2D web guidelines. Digital video captioning involves the placement of text originating from a solitary audio source in a stationary location on a display. However, the provision of captions in immersive spaces necessitates the captioning of multiple audio sources within a 3D setting. The process of enhancing the accessibility of 2D web pages for screen readers is comparatively simpler than achieving the same in a setting where most of the elements are rendered digitally in 3D space. The absence of established accessibility standards or commonly accepted best practices for AR/VR

[124] Ibid.
[125] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[126] Joshue O Connor et. al, 'XR Accessibility User Requirements' (*W3C Working Draft,* 16 September 2020) <https://wwww3.org/TR/xaur> accessed 29 May 2023.

technology implies that developers frequently create and integrate accessibility features from scratch, which can be a resource-intensive and time-consuming undertaking. This may potentially dissuade developers from prioritizing accessibility in their initial design process.

In addition, proficiency in operating AR/VR equipment and traversing simulated environments is deemed a fundamental prerequisite. However, inclusive design unaccompanied by other measures is insufficient in surmounting the obstacles to acceptance that disproportionately affect susceptible, marginalized, and underprivileged users. The phenomenon commonly referred to as the "digital divide" has been extensively documented. It pertains to the tendency for marginalized and underserved communities to be excluded from technological advancements, particularly in the early stages of their development.

Consequently, the result is a reduction in the general acceptance levels among prospective users who stand to gain from such technologies, such as individuals from low-income and rural communities, elderly individuals, and those with disabilities across all age groups. The existing disparities in fundamental Internet and digital communications may have implications for the equitable adoption of AR/VR technology. Larry Goldberg has noted that the utilization of technology that necessitates high-speed broadband and sophisticated hardware could potentially exacerbate this divide.[127] The widespread adoption and access of both stationary and mobile AR/VR solutions necessitate robust wireless or high-speed Internet connections. While certain rudimentary immersive experiences, such as 360-degree videos that are locally stored and other single-user applications, may not necessitate an Internet connection, most advanced functionalities, particularly those that employ AR/VR technologies to augment collaboration and communication, mandate a dependable and high-speed connection. The increasing positivity surrounding the potential of AR/VR is closely linked to the progress made in 5G technology. This development would enable compact wearable devices, such as smart glasses, to transfer processing capabilities to cloud servers without compromising the user's experience or depending on autonomous internet connections.[128] However, the adoption of high-speed Internet remains low among many potential users, particularly those residing in rural and low-income communities.

[127] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 29 May 2023.
[128] Robert Cheng, 'Can 5G Make Smart Glasses Cool?' (*Cnet,* 1 March 2018) <https://www.cnet.com/news/can-5g-make-smart-glasses-cool-ericsson-odg-mwc-2018.> accessed 29 May 2023.

According to a study conducted by the Pew Research Center in 2018, individuals residing in rural areas exhibited lower rates of Internet usage, smartphone ownership, and home broadband subscription in comparison to their urban and suburban counterparts.[129] To fully leverage the capabilities of AR/VR technology in mitigating the challenges posed by geographical separation, it is imperative for policymakers to guarantee the availability of broadband that is capable of supporting remote work, telehealth, and assistive technology applications to a significant proportion of the populace. Furthermore, the affordability of such broadband services should be ensured for all individuals, irrespective of their income levels.[130] Incorporating well-crafted subsidies to facilitate the expansion and uptake of broadband services is a fundamental element that ought to be integrated into prospective legislation geared towards enhancing the infrastructure of the countries.

Despite the rapid pace of innovation in the development of more accessible and intuitive AR/VR technologies, the expense associated with the acquisition of such devices continues to pose a significant barrier for a considerable portion of the population. The most economical alternatives available to users in the domains of AR and VR are applications that are either mobile-based or web-based. However, it should be noted that the utilization of these technologies necessitates the possession of a smartphone or other mobile device that is compatible, as well as a personal computer. Additionally, it is worth mentioning that the functionalities of mobile-tethered applications are frequently constrained.[131] In 2019, the cost of VR headsets not dependent on a mobile device varied from approximately $250 to $1,000 per individual unit.[132] The expenses associated with wearable heads-up displays, such as smart glasses and mixed reality headsets, continue to be relatively elevated.[133] The cost of VR solutions may be a hindrance for individual users and smaller organizations that contemplate

[129] Monica Anderson, 'About a Quarter of Rural Americans Say Access to High-Speed Internet is a Major Problem' (*Pew Research Center*, 10 September 2018) <https://www.pewresearch.org/fact-tank/2018/09/10/about-a-quarter-of-rural-americans-say-access-to-high-speed-internet-is-a-major-problem.> accessed 29 May 2023.

[130] Doug Brake and Alexandra Bruer, 'How to Bridge the Rural Broadband Gap Once and for All' (*Information Technology and Innovation Foundation*, 22 March 2021) <https://itif.org/publications/2021/03/22/how-bridge-rural-broadband-gap-once-and-all/> accessed 29 May 2023.

[131] Signe Brewster, 'The Best VR Headset: But What About Mobile VR?' (*The New York Times*, 3 November 2020) <https://www.nytimes.com/wirecutter/reviews/best-standalone-vr-headset/#what-about-mobile-vr.> accessed 29 May 2023.

[132] Lionel Sujay Valishery, 'Reported Price of Leading Consumer Virtual Reality (VR) Headsets in 2019, by Device' (*statista*, 22 January 2021) <https://www.statista.com/statistics/1096886/reported-price-of-leading-consumer-vr-headsets-by-device.> accessed 30 May 2023.

[133] Samantha Subin, 'Is 2021 Finally the Year for Smart Glasses? Here's Why Some Experts Still Say No' (*CNBC*, 23 January 2021) <https://www.cnbc.com/2021/01/23/why-experts-dont-expect-smart-glasses-to-surge-in-2021.html.> accessed 30 May 2023.

its adoption, potentially exacerbating the digital divide for those who could otherwise reap the benefits of this technology. Currently, universal access to AR/VR devices is not imperative. However, it may prove advantageous to facilitate access for institutions catering to specific demographics, such as schools primarily serving underprivileged students. These obstacles may give rise to intangible yet equally significant impediments to knowledge acquisition. The delay in the adoption of technology is often accompanied by a corresponding deficiency in technical proficiency and self-assurance with respect to novel advancements. Certain gaps in knowledge can be attributed to generational differences.

According to a survey conducted by the Pew Research Centre in 2015, individuals in the United States who are over the age of 65 are more prone to experiencing low levels of confidence when utilizing digital tools, often requiring assistance when configuring new devices.[134] Nonetheless, there are digital literacy disparities prevalent among several vulnerable and marginalized communities that could potentially benefit from the utilization of AR/VR technologies. A survey conducted by the Pew Research Centre on digital readiness for online learning revealed that approximately 50% of adults in the US exhibited a degree of reluctance towards adopting these technologies. The survey also indicated that women, individuals with lower levels of formal education, members of lower-income households, and individuals aged 50 and over were more likely to exhibit this reluctance.[135]

Whilst AR/VR devices and applications may present novel and distinctive features to most users, their underlying principles are derived from pre-existing digital technologies. The existence of persistent gaps in digital knowledge can place underrepresented users at a disadvantage from the outset, which may lead to a decrease in overall usage or increased vulnerability to potential harms resulting from incorrect usage. The incorporation of user education and digital literacy will play a crucial role in the implementation of equity and inclusion initiatives driven by AR and VR. It is imperative to acknowledge that numerous hindrances to the adoption of a particular technology or service exist concurrently for numerous prospective users. These hindrances act as amplifiers that can intensify inequalities in accessibility. As stated by Lydia X.Z. Brown from the Centre for Democracy and Technology,

[134] Monica Anderson and Andrew Perrin, 'Tech Adoption Climbs Among Older Adults: Barriers to Adoption and Attitudes Towards Technology' (*Pew Research Center,* May 17, 2017) <https://www.pewresearch.org/internet/2017/05/17/barriers-to-adoption-and-attitudes-towards-technology.> accessed 30 May 2023.

[135] John B Horrigan, 'Digital Readiness Gaps' (*Pew Research Center,* 20 September 2016) <https://www.pewresearch.org/internet/2016/09/20/digital-readiness-gaps.> accessed 30 May 2023.

individuals with disabilities exhibit a higher likelihood of experiencing unemployment and underemployment, as well as a greater likelihood of living in poverty. The reduced probability of obtaining dependable broadband connectivity and access to technological devices is a concern.[136] This issue is particularly relevant for a considerable proportion of the American population with disabilities, who are also older adults. Inadequate levels of digital proficiency may further compound the difficulties posed by inaccessible design.[137] Consequently, endeavours that solely address specific impediments to accessibility will inevitably fail to encompass a significant number of communities.

Ultimately, the development of inclusive AR and VR technologies should encompass not only the provision of fair and impartial access, but also the creation of immersive experiences that are inclusive in nature. The utilization of a singular default, typically representing a white male,[138]and able-bodied individual, in AR/VR experiences may potentially dissuade prospective users who do not identify with or relate to this default from engaging in immersive experiences to their fullest extent. As per the account of a participant in the study concerning women in social VR, the sole source of discomfort arises from the initial avatar representation of a balding Caucasian male. The consideration of diverse user needs and preferences is crucial in the design of AR/VR solutions to ensure that they are at least as inclusive as their real-world counterparts. This is particularly important to avoid the exclusion of individuals who do not conform to the stereotypical image of a balding white male. With the increasing prevalence of these technologies among consumers, AR/VR platforms and services have implemented more comprehensive methods for avatar selection. These methods encompass a spectrum of options, ranging from representations that closely resemble reality to those that offer extensive customization. In practical settings, individuals tend to modify their attire and conduct in accordance with the situational demands, for instance, exhibiting distinct behaviours at a formal conference as opposed to a relaxed social gathering with acquaintances. The ability to control one's interaction and representation within immersive experiences is crucial for AR/VR technologies to effectively replicate and enhance physical spaces. April Boyd-Noronha, the

[136] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 30 May 2023.

[137] Monica Anderson and Andrew Perrin, 'Disabled Americans are Less Likely to Use Technology' (*Pew Research Center,* 7 April 2017) <https://www.pewresearch.org/fact-tank/2017/04/07/disabled-americans-are-less-likely-to-use-technology.> accessed 30 May 2023.

[138] Jessica Outlaw and Duckles, 'Why Women Don't Like Virtual Reality: A Study of Safety, Useability, and Self-Expression in Social VR' (*The Extended Mind*) <https://static1.squarespace.com/static/60e8ceb4ae52881d57698bf6/t/6164b95156a52d3614c29e82/1633990999726/The-Extended-Mind_Why-Women-Don%27t-Like-Social-VR_2017.pdf> accessed 30 May 2023.

leader of the Cyber XR Coalition, an organization that promotes inclusive AR/VR,[139] stated that individuals possess ownership of their identity, yet desire the ability to modify it or portray themselves in any desired manner. Boyd-Noronha is an expert in diversity, equity, and inclusion. This assertion holds significant weight for individuals who belong to marginalized and underrepresented groups. Such individuals may seek to convey visual markers of their identity in their virtual and physical surroundings, or alternatively, may wish to conceal these attributes in order to safeguard their privacy and well-being.[140]

According to Dylan Fox, an advisor for the XR Access Initiative, the decision of whether to disclose one's disability is significant for individuals with disabilities. The inclusion of avatars with wheelchairs in certain contexts may be deemed necessary, while in other situations it may not be deemed as such.[141] The incorporation of diverse representation within immersive experiences is bound to entail certain compromises. Individuals have the option to present themselves with a race, gender, or disability that differs from their actual identity in the physical world. However, certain individuals may choose to do so with the intention of causing disruption, such as ridiculing individuals with disabilities or perpetuating racial stereotypes. Alternatively, virtual spaces may necessitate the disclosure of marginalized identities or the erasure of such identities altogether.[142] The absence of proper representation and mandatory disclosure in AR/VR technology could potentially reduce its appeal and hinder its adoption for personal or social purposes. However, this issue raises significant concerns for other use cases, such as workplace or educational applications.[143] Developers who are constructing immersive experiences for multiple users should prioritize the implementation of codes of conduct, as well as monitoring and enforcement mechanisms that effectively discourage instances of malicious misrepresentation.

[139] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 30 May 2023.
[140] Ibid.
[141] Ibid.
[142] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 31 May 2023.
[143] Ibid.

2.5.1.3. RISKS AND CHALLENGES OF BIAS & DISCRIMINATION FOR VULNERABLE USERS IN AR/VR

The most significant potential of AR and VR lies in its capacity to depict the tangible world in a partially or completely simulated environment. Nevertheless, it is noteworthy that the VRs may also reflect the biases that are present in the real world. According to April Boyd-Noronha, discrimination based on race and gender, commonly referred to as "isms," is not limited to the physical world and can also manifest in VR environments.[144] Although AR/VR technologies have the potential to function as instruments in mitigating bias, it is crucial to contemplate the manners in which AR/VR devices may reproduce or intensify detrimental discrimination within virtual encounters. By acknowledging the risks, developers and implementing organisations can formulate appropriate policies, practises, and technical mechanisms to mitigate the likelihood of real-world bias and discrimination impeding the efficacy of multi-user immersive experiences.

Certain apprehensions arise from social interactions. According to VR researcher Jessica Outlaw, social VR environments are built upon distinct cultural norms and behaviours, like any other social group. These cultural elements include heroes, archetypes, and mascots, as well as stories, myths, and origin stories. Additionally, ceremonies, rituals, symbolic acts, and rites of passage are present, along with symbols, language, artefacts, taboos, and jokes.[145] Underrepresented individuals who are prone to bias and discrimination are often excluded from virtual spaces, resulting in the development of key elements that cater to a specific user base, typically consisting of white males. The circumstance has the potential to result in discriminatory practises, albeit unintentionally, within said environments. Jessica Outlaw pointed out that if one's heroes only represent a single demographic, it raises questions about the inclusivity and accessibility of the space being created. Specifically, it prompts consideration of the intended audience and the individuals who are invited to participate.[146]

Undoubtedly, biases that are both explicit and implicit, and are rooted in visual appearance, will continue to exist in virtual environments, which are employed for various purposes such as education, employment, healthcare, and other services. In certain cases, users may opt for

[144] Ibid.
[145] Kent Bye and Jessica Outlaw, 'Elements of Culture and Cultivating Community with Jessica Outlaw' (*Voices of VR Podcast*, 6 July 2019) <http://voicesofvr.com/784-elements-of-culture-cultivating-community-with-jessica-outlaw.> accessed 31 May 2023.
[146] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation*, 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 31 May 2023.

or necessitate the use of avatars that are photorealistic or closely resembling reality, thereby rendering it arduous to conceal aspects of their identity such as gender and race. Apart from managing the partialities of colleagues, practitioners, and associates, individuals may also carry their own internalised prejudices into these domains. Empirical research indicates that individuals tend to internalise preconceived notions regarding their anticipated level of performance, which are often influenced by their racial identity.[147] The extent to which self-stereotyping is reinforced, mitigated, or remains unaffected when users adopt an avatar possessing identical characteristics is yet to be determined.[148]

AR/VR has the potential to perpetuate pre-existing biases within virtual environments, as well as exacerbate discriminatory attitudes and behaviours in the physical world. The correlation between the apprehensions of safety, accessibility, and inclusive design addressed and the possibility of AR/VR exacerbating discrimination in people's everyday experiences is undeniable. The collection and interpretation of user data in AR/VR environments may potentially expose sensitive personal information, such as race, gender, disability, age, or sexuality, thereby increasing the risk of discriminatory practises.[149] Moreover, the utilisation of AR/VR assessments in the recruitment process may lead to discriminatory outcomes for candidates who exhibit suboptimal performance owing to issues related to accessibility, discomfort, inadequate comprehension of the technology, or a viewpoint that was not considered during the development of the experience.[150] Despite ongoing advancements in these tools, there exists empirical evidence suggesting that certain criteria's employed in pre-screening hiring technologies fail to adequately consider a wide range of candidates, particularly individuals with disabilities.

Instances of de facto discrimination may manifest within work environments, academic settings, and other domains that implement AR/VR technologies, as individuals who are incapable of utilising such devices may be excluded from engaging in beneficial activities, such

[147] Ebony McGee, 'Black Genius, Asian Fail: The Detriment of Stereotype Lift and Stereotype Threat in High-Achieving Asian and Black STEM Students' (*AERA Open*, 5 December 2018), <https://doi.org/10.1177%2F2332858418816658.> accessed 31 May 2023.
[148] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 31 May 2023.
[149] Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology & Innovation Foundation,* 4 March 2021) < https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 31 May 2023.
[150] Lydia X.Z. Brown et. al, 'Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?' (*Center for Democracy and Technology,* 3 December 2020) <https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination.> accessed 31May 2023.

as educational sessions or collaborative gatherings.[151] The disparity in access may have implications for prospects of progression, career growth, and academic enhancement. Cynthia Bennett, a scholar from Carnegie Mellon University, expressed apprehension regarding the potential adoption of these technologies by educational institutions and public access museums. She posited that such a move could result in limited accessibility to these technologies, thereby creating disparities in access to public and business spaces, as well as in education.[152] It is imperative to uphold tangible alternatives to digital environments that are both accessible and captivating.

2.5.2 CONCEPT OF BIOMETRIC PSYCHOGRAPHY AND ITS POTENTIAL IMPLICATIONS FOR PRIVACY INFRINGEMENT

The field of immersive technology presents a considerable potential for human rights violations, particularly in the area of biometric data and its associated limitations. This phenomenon can be attributed to the nature of the data that is capable of being accumulated, as well as a fundamental incongruity with the existing legal framework. The correlation between biometric data and biometric identifiers, as conventionally delineated, and the technological capabilities and possible risks of immersive technologies is not a simple matter.

The present legal delineations of biometric data in countries such as the USA inadequately address the progressions in immersive technologies. The phenomenon can be attributed to a multitude of factors, including but not limited to the hardware features at one's disposal, their corresponding functionalities, the user data that can be extracted, and the potential applications of said data. As of November 2019, legislation pertaining to the handling and usage of biometric data was present in three states within the USA. The CCPA will be enforced in California starting from January 1, 2020. Several states are currently considering legislation related to biometrics.[153]

The Illinois Biometric Information Privacy Act is the most all-encompassing and legally disputed regulation concerning biometrics within the United States. The legislation in the state

[151] 'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (XR Association, October 2020) <https://xra.org/wpcontent/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 31 May 2023.
[152] Ellysse Dick, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 31May 2023.
[153] Molly K. McGinley et. al, 'The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States' (2023) XIII THE NATIONAL LAW REVIEW <https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states> accessed 31 May 2023.

of Illinois delineates two discrete and independent definitions for the concepts of "biometric identifier" and "biometric information."[154] In accordance with this law, a "biometric identifier" pertains to a physical trait or characteristic that possesses the capacity to distinguish an individual from others in a singular and distinctive manner. The term refers to a biometric modality that encompasses the scanning of a retina or iris, fingerprint, voiceprint, or the geometry of a hand or face.[155] The scope of biometric identifier is limited to specific data types and excludes certain categories such as demographic data, physical descriptions, photographs, written signatures, writing samples, tattoo descriptions, and human biological samples that are used for legitimate scientific testing or screening. Furthermore, the definition of excluded materials encompasses biological substances or data collected within a medical setting.[156] In accordance with the statute, the phrase "biometric information" encompasses all information that pertains to the biometric identifier of an individual, regardless of the means by which it was obtained, transformed, retained, or distributed. It is noteworthy that the definition of biometric identifiers specifically excludes data that is obtained from techniques or objects that fall outside the purview of biometric identifiers.[157] The legal provision provides protection for both biometric identifiers and biometric data.[158] The operational characteristics of hardware may bear consequences for the implementation of the statute. The definition of the Illinois law is a two-step process, which results in uncertainty regarding the extent to which the law's safeguards apply to facial recognition software that detects faces from images. Facial geometry scans are categorized as biometric identifiers, whereas photographs are not encompassed within the roster of biometric identifiers. Moreover, it should be noted that data that is derived from an excluded source cannot be classified as "biometric information."

The introduction of new technological developments is expected to introduce further intricacies and ambiguities. At present, controller-free mechanisms for VR are at the forefront of potential applications.[159] The situation leads to an untested legal domain, and the outcome may vary depending on the methodology used to produce scans of "hand geometry" that assist users in creating their unique interface. Now, is it possible for a court of law to ascertain whether the

[154] 740 ILL. COMP. STAT. ANN. 14/10 <http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57> accessed 31 May 2023.
[155] Ibid.
[156] Ibid.
[157] Ibid.
[158] 740 ILL. COMP. STAT. ANN. 14/15
[159] Meta Quest Blog, 'Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR' (*Meta*, 25 September 2019) <https://www.oculus.com/blog/introducinghand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed 31 May 2023.

act of linking this data to a user's Facebook or Oculus account amounts to identification? Could the measurement of the hand be regarded as a physical characteristic like height or weight, thus disqualifying it from being incorporated into the definition? Ensuring consistency of technology across diverse platforms cannot be assured, thus creating the potential for incongruous results if determinations are made solely based on control type rather than technical specifications.

Moreover, two state-level statutes in the United States, specifically in Texas and Washington,[160] have been enacted with the specific purpose of protecting biometric privacy. Both measures are designed with the specific purpose of restricting the collection of biometric data for commercial purposes. The definition of "biometric identifier" in the Texas legislation is like that of the Illinois statute, as it includes a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.[161] The Washington statute defines "biometric identifier" in a comprehensive manner, which includes data that is automatically produced by measuring an individual's biological traits. This encompasses a range of distinct biological patterns or characteristics, such as fingerprints, voiceprints, eye retinas, irises, and others, that are utilised for the purpose of identifying a specific individual.[162] The definition "biometric identifier" has a limited scope and does not encompass specific items such as digital or physical photographs, audio or video recordings, or any data that is obtained, utilized, or stored for healthcare treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.[163]

The state of Delaware has also incorporated "biometric data" into a list of personal information that is protected by a comprehensive data security regulation. The aforementioned regulation pertains exclusively to biometric data that is distinct and produced through the measurement or analysis of human body characteristics for the purpose of authentication.[164] The proposed federal statute, which seeks to improve the overall protection of personal information, is similar to the legislation in Illinois and defines "biometric information" as including a retina or iris

[160] The inclusion of this area within the purview of the California Consumer Privacy Act (CCPA) will be facilitated through its incorporation into a comprehensive privacy legislation. At present, the means by which the bill will be enforced remains uncertain, rendering it peripheral to the present analysis.
[161] TEX. BUS & COMM. § 503.010.
[162] WASH. REV. CODE § 19.35.010.
[163] Ibid.
[164] The Delaware statute serves as an illustrative instance of a definition for biometric data. However, it is important to note that the statute primarily pertains to data breach notification obligations rather than the handling of biometric information. Consequently, I will not further delve into its specifics. 6 DEL. C. § 12B-101.

scan, fingerprint, voiceprint, or scan of hand or face geometry.[165] Broadly speaking, the deployment of biometric security measures at the state level is centred around the concept of authenticating identity by means of physiological attributes. Each of the provided definitions includes two constraints that are embedded within. At the outset, there is a dependence on restricted physiological categorizations of data that may not encompass insights derived from immersive systems. Furthermore, it is imperative to acknowledge that the data is exclusively incorporated if it is considered essential for authentication purposes. The second constraint exhibits a notable deficiency within the system. It is improbable that physiological information related to an individual's preferences, tendencies, or motivations, rather than their personal identity, is subject to protection. While non-immersive technologies may have limited potential for data capture, immersive environments with their advanced data capture capabilities offer ample opportunities for utilizing data in this way.

In addition, let us discuss the term "biometric psychography" as proposed by Brittan Heller in her article.[166] The concept of "biometric psychography" denotes a novel type of corporeal-based data that is differentiated from identity and concerns an individual's preferences. The term referred to above refers to the combination of behavioural and anatomical information that is used to identify or quantify an individual's response to stimuli over a specific duration. The data provides significant perspectives on an individual's physiological, psychological, and affective condition, along with their domains of inclination. The term "biometric psychography" is an integration of biometric and psychographic data. Here 'psychographic data' a concept derived from the field of advertising, which involves quantifiable measures that appraise an individual's cognitive characteristics, including emotions, values, and attitudes, in order to assess their behaviours, preferences, and viewpoints.[167] Whereas, one may consider biometrics as a set of static visual representations that capture unique fingerprint patterns, thereby establishing an individual's distinctiveness and personal identity. On the other hand, psychographics bear resemblance to consumer profiles that delineate an individual's proclivities towards purchasing or shifts in attitudes over a specified duration. The differentiation is of considerable importance owing to the inherent characteristics and possible consequences of the information that could be contained in biometric psychographics.

[165] S.1214, § 2(10)(B)(iv).
[166] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed on 31 May 2023.
[167] Ibid.

Notwithstanding its constraints, extant legal and scholarly frameworks exist to regulate and assess the impacts of biometric technologies that centre on conventional identity indicators. At present, there exists an insufficiency of data pertaining to the prospective ramifications of biometric psychography. What type of information is typically included in the classification of biometric psychographics? One facet concerns biological data that can be classified as either biometric information or biometric identifiers. Upon analysing immersive technologies, it is plausible that biometric tracking techniques may be categorized as such, contingent upon the legal statutes and regulations of the jurisdiction under consideration.

The present investigation centres on the examination of eye tracking and pupillometry. Facial scanning is a biometric modality that utilizes algorithms to analyse and identify distinct facial characteristics for the purpose of identification. GSR[168] is a physiological process that quantifies the electrical conductance of the skin when exposed to physiological or emotional stimuli. The three diagnostic techniques being evaluated are EEG, EMG, and ECG,[169] all of which are medical in nature. The measurements exhibit a more profound significance than their surface-level interpretation. To elaborate, the application of facial tracking technology holds promise in predicting an individual's emotional states. Facial muscle movements can serve as a means of identifying seven distinct emotions, including anger, surprise, fear, joy, sadness, contempt, or disgust, which exhibit a high degree of correlation.[170] EEG is a neurophysiological method that identifies and documents cerebral electrical activity, as manifested by the presence of brain waves. The analysis of brain waves can offer valuable information regarding an individual's cognitive and emotional conditions. The utilization of EEG has the potential to offer valuable insights into an individual's cognitive load. What is the degree of unpleasantness or frequency of occurrence linked to a particular task? What is the cognitive workload level associated with a particular task?[171] GSR is a physiological indicator that reflects the magnitude of an individual's emotional condition, such as stress or anxiety. This metric is frequently utilized in polygraph examinations for the purpose of detecting deception.[172] EMG can quantify muscle tension, facilitating the identification of micro-expressions that may pose a challenge

[168] Galvanic skin response refers to the alteration in the skin's electrical resistance resulting from emotional stress, which can be quantified using a highly sensitive galvanometer. Lie-detector tests commonly employ this technique.
[169] '#517: Biometric Data Streams & the Unknown Ethical Threshold of Predicting & Controlling Behaviour' (*Voices of VR Podcast*, 20 March 2017) <http:// voicesofvr.com/517-biometric-data-streams-the-unknown-ethical-threshold-of-predicting-controlling-behavior/> accessed 31 May 2023.
[170] Ibid.
[171] Ibid.
[172] Ibid.

for individuals to deliberately regulate, thus exposing automatic responses.[173] This tool is deemed invaluable for determining the truthfulness of individuals' assertions. ECG has the potential to function as a reliable measure of truthfulness, as it allows for the monitoring of alterations in an individual's heart rate or blood pressure in reaction to a specific stimulus.[174]

The differentiation between biometric psychography and biometric data pertains to the former's capacity to not only reveal an individual's present physiological and/or affective state, but also to ascertain the external stimuli that are provoking such responses. The data possesses the capability to not only unveil an individual's identity, but also their perceptual and affective reactions to diverse stimuli, and facilitate deductions founded on the temporal oscillations in their physiological condition. This statement suggests that it has the potential to offer valuable information regarding an individual's concentration and the corresponding emotional significance. The amalgamation of biological observations and eye tracking can aid in the recording of an individual's reactions and stimuli, thereby providing a more concrete illustration. In the context of a VR game, it is possible for an individual to exhibit an elevated level of excitement when presented with a new red car. The act of vehicular observation elicits a physiological response of hedonic pleasure from the human body. Let us contemplate a hypothetical situation where the data is sold to marketers, who then proceed to inundate your digital interactions with promotional content related to the previously mentioned automobile. The potential of immersive technologies lies in their ability to measure and retain biometric information beyond the legal framework that focuses on biometric identifiers. Immersive technologies are not limited to static measurements or images, as they integrate sensors that continuously monitor users' movements in space for a prolonged period. Furthermore, the individuals consistently record changes in the surrounding environment and the possible consequences of such modifications on the user's condition in the future. The VR/AR platforms have the capability to access not only the user's genuine identity but also their financial and account details. The term in question pertains to a new type of data that incorporates an individual's genuine identity in combination with diverse stimuli, thus mirroring their unique cognitions, inclinations, and aspirations.

The topic of eye tracking and pupillometry serves as an illustrative example. The utilization of eye tracking and pupil dilation measurements is a crucial aspect of biometric psychography. Eye tracking is an anatomical measurement technique that entails observing the eye's

[173] Ibid.
[174] Ibid.

movement and focus to ascertain the visual stimuli that an individual is attending to. The field of pupillometry is dedicated to examining changes in pupil size as they relate to cognitive processing.[175] This enables scholars to investigate diverse facets of human cognition, including perception, language comprehension, memory consolidation, decision-making, emotional reactions, and cognitive development.[176] Pupillometry is a specialized area of study that focuses on investigating the physiological reactions of the pupil to different types of stimuli, encompassing both its dilation and contraction responses. The collected measurements serve to monitor changes in an individual's physical state over a given duration. In a virtual reality environment, the data obtained using an HMD will not solely record the user's behaviours, but also the stimuli that may have influenced said behaviours. This statement implies that users' visual attention can be influenced by the salience of stimuli, the duration of fixation, the level of attention given to a specific object or event, and the path of their gaze. In summary, the expansion of the pupils possesses the capacity to serve as an involuntary affirmative reaction, akin to the operation of a digital "like" feature.[177]

What is the underlying mechanism that governs this process? The technique of tracking the visual fixation and ocular position of individuals is frequently accomplished by employing projectors that produce a near-infrared illumination design on the user's eyes. The proposed technique entails the acquisition of high-speed visual recordings of both the illumination patterns and the ocular structures of the individual. Algorithms are employed for the purpose of processing patterns, wherein the images are scrutinized to ascertain the location of the eyes and the focal point of the gaze.[178] Through the integration of this data with the measurement of nuanced facial muscle movements and changes in pupil dilation, it becomes feasible to evaluate an individual's emotional reactions.[179]

Most eye tracking methods involve the use of an IR and a camera aimed at the eye, from a technical perspective. The application of IR is employed for the purpose of illuminating the eye. Subsequently, an IR-sensitive camera is utilized to analyse the reflections. The wavelength of the light is commonly measured at 850 nanometres. It exists outside the observable spectrum

[175] Sylvain Sirois & Julie Brisson, 'Pupillometry' (2014) 5 Wires Cognitive Science <https://onlinelibrary.wiley.com/doi/abs/10.1002/wcs.1323> 679–692.
[176] Bryn Farnsworth, 'Pupillometry 101: What You Need to Know' (*IMOTIONS*) <https://imotions.com/blog/pupillometry-101/> accessed 1 June 2023.
[177] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail' (*VICE*, 28 May 2019) < https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 1 June 2023.
[178] Ibid.
[179] Ibid.

of electromagnetic radiation that falls between 390 and 700 nanometres in wavelength. Whereas the human eye lacks the capacity to detect luminance, the camera possesses the capability to perceive it. The phenomenon of visual perception encompasses the identification of luminous stimuli penetrating the pupil via the retinal mechanism. Furthermore, the student functions as an entrance for IR to penetrate the ocular organ. Light cannot enter the eye beyond the pupil. Conversely, it demonstrates retroreflection in the direction of the imaging apparatus. The camera detects the pupil as an area with no reflection, leading to a dark region, whereas the rest of the eye displays a brighter appearance. The nomenclature under discussion pertains to the technique of "dark pupil eye tracking." If the IR light source is placed near the optical axis, it may reflect off the back of the eye and the individual in question demonstrates a notable degree of cognitive ability. The term "bright pupil eye tracking" is commonly used in academic discourse to refer to these phenomena. Analogous to the occurrence of the "red eye" phenomenon that is discernible in flash photography. Irrespective of the utilization of a dark or bright pupil, the essential factor is that the pupil demonstrates disparities from the adjacent ocular tissue. The image that has been obtained is then subjected to a series of processing steps to determine the exact location of the pupil. This facilitates the computation of the gaze orientation through the analysis of ocular observations. The process of executing processing tasks can be carried out on a diverse range of devices, including personal computers, mobile phones, or other interconnected processors. Various vendors have developed specialized chips that can alleviate the primary CPU of its processing responsibilities. The integration of gaze measurements from both eyes can be achieved through the utilization of eye-tracking cameras that capture data from each eye. This enables the determination of the user's point of fixation in a 3D environment, whether it is real or virtual.[180]

The incorporation of eye tracking technology is an increasingly significant element within the realm of VR.[181] The nascent enterprise provides eye tracking equipment specifically tailored for software developers. Tobii was unveiled to considerable acclaim in January 2018 and is currently in active deployment. Tobii provides a range of products, one of which is a developer's kit for eye tracking that is compatible with multiple platforms and supports various programming languages. The Tobi G2OM is a machine learning algorithm that exhibits

[180] 'How Does Eye Tracking Work?' (*VR.org*, 22 February 2018) <https://www.vr.org/2018/02/22/how-does-eye-tracking-work/> accessed 1 June 2023.
[181] Ed Klaris & Alexia Bedat, 'VR & AR: Virtual Reality, Augmented Reality & Biometric Data after 2017-Ed Klaris & Alexia Bedat' (*MEDIUM*, 1 February 2018) <https://blog.klarislaw.com/vr-ar-virtual-reality-augmented-reality-biometric-data-after-2017-ed-klaris-alexia-bedat-a15e9cb000a1> accessed 1 June 2023.

considerable interest for our objectives, as it demonstrates the ability to accurately forecast the user's visual focus.[182] Both Microsoft Hololens and Magic Leap encourage third-party developers to create applications that utilize eye tracking data.[183] The utility of eye tracking surpasses the realm of biometric psychography. It is essential to acknowledge that the implementation of foveated rendering, a critical element in enhancing immersive experiences, requires the incorporation of eye tracking technology. This is due to its capability to facilitate the identification of regions that necessitate improvement or obscuring, contingent on the user's visual focus.[184]

The utilization of eye tracking and pupil dilation monitoring as indicators of visual salience can provide insights beyond basic identification, thus prompting concerns related to user privacy, human rights, and the possibility of self-censorship. The measurement of pupil dilation holds promise for uncovering various implications, such as an individual's sexual attraction and susceptibility to developing illnesses such as dementia. HMDs that are integrated with eye-tracking functionalities possess the capacity to offer significant insights to advertisers. HMDs have the capability to gather data that was previously only accessible through laboratory experiments by monitoring users' gaze, attention span, and emotional reactions to visual stimuli. The hypothetical capacity to perceive thoughts has the potential to transform the fundamental essence of technology, inducing individuals to practice self-regulation of their innermost thoughts, sentiments, and affective states.

[182] Tobii Homepage, (*Tobii*) < https://developer.tobii.com/xr/> accessed 1 June 2023.
[183] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail' (*VICE*, 28 May 2019) <https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 1 June 2023.
[184] Jeremy Horwitz, 'HTC Vive Pro Eye hands-on: Gaze into VR's future with foveated rendering' (*Venturebeat*, 10 January 2019) <https://venturebeat.com/2019/01/10/htc-vivepro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 1 June 2023.

CHAPTER 3

PRIVACY & DATA PROTECTION IN IMMERSIVE TECHNOLOGIES

3.1. RIGHT TO PRIVACY UNDER INTERNATIONAL HUMAN RIGHTS LAW

Before discussion about the Privacy and Data Protection issues under Immersive Technologies, let us first have an idea about the Right to Privacy as an important right under International Human Rights Law and as a right in a democratic nation (in this case). Then let us discuss a little bit about Data Protection and its importance as a human right.

The right to privacy is a crucial aspect of individual autonomy and the safeguarding of human dignity, constituting a fundamental cornerstone upon which numerous other human rights are predicated. The concept of privacy facilitates the establishment of boundaries and the management of barriers to safeguard against unjustified intrusion into our personal lives. This, in turn, affords us the opportunity to determine our identity and dictate our interactions with the external environment. The concept of privacy serves to demarcate boundaries that restrict the individuals or entities that may gain access to our physical spaces, possessions, and communication channels, as well as our personal information. Privacy regulations provide individuals with the capacity to assert their rights in the presence of substantial power differentials. The safeguarding of privacy is a crucial measure employed to shield individuals and the community at large from unwarranted and capricious exercise of authority. This is achieved by limiting the extent of information that can be obtained about us and the actions that can be taken against us, while simultaneously shielding us from external forces that may seek to impose their influence. The concept of privacy is fundamental to the human identity, and individuals are faced with choices regarding it daily. The provision of a non-judgmental space enables individuals to express themselves freely without fear of prejudice, fostering independent thought and affording individuals agency over the dissemination of their personal information.

The discourse surrounding privacy in contemporary society pertains to the discussion of contemporary liberties. As we contemplate the establishment and safeguarding of boundaries pertaining to the individual, as well as the individual's agency in determining their fate, we are simultaneously grappling with the following question. This discourse pertains to the ethical considerations that arise in contemporary society, the regulations that dictate the behaviour of commercial activities, and the limitations imposed on the authority of governmental institutions. The right in question has consistently been intertwined with technology. Currently,

there exists an unprecedented capacity for surveillance, while conversely, the ability to safeguard privacy has reached an all-time high. It is now possible to distinguish individuals with precision within large sets of data and streams, and to make decisions regarding individuals based on extensive amounts of data. Presently, corporations and governmental entities have the capacity to oversee all our dialogues, commercial dealings, and physical movements. The capabilities possess the potential to yield adverse consequences for individuals, groups, and society at large, as they may engender a sense of inhibition, exclusion, and discrimination. Moreover, they exert an influence on our cognitive processes regarding the interconnections among the individual, markets, society, and the state. If institutions possess the capability to gain comprehensive knowledge of individuals, including their past actions, present behaviour, and future conduct, it is likely that significant power differentials will arise. This could result in the erosion of individual autonomy in the face of entities such as corporations, collectives, and governments.[185]

Furthermore, any behaviour deemed deviant may be detected, ostracised, and potentially suppressed. One of the foremost obstacles to privacy pertains to the potential for the right to be infringed upon without the individual's knowledge. In regards to various entitlements, one is cognizant of the potential for intervention, such as apprehension, censorship, or confinement. In addition to other entitlements, one must also take into consideration the perpetrator, which may include the apprehending authority, the censoring entity, or law enforcement personnel. There is a growing trend of insufficient disclosure regarding the surveillance measures imposed upon individuals, coupled with a lack of resources and avenues for inquiry to scrutinise these practises. The practise of covert surveillance, which was previously limited due to its intrusive nature, lack of transparency, and potential threat to democratic principles, is rapidly becoming the norm. Privacy International's vision is to establish a global society where privacy is safeguarded, esteemed, and realised. There is a growing trend among institutions to implement surveillance measures, which often result in individuals being excluded from participating in decisions pertaining to the processing of their personal information, scrutiny of their bodies, and search of their possessions. It is our contention that the ability of individuals to fully engage in contemporary society is contingent upon advancements in legal and technological

[185] 'What is Privacy' (Privacy International, 23 October 2017) <https://privacyinternational.org/explainer/56/what-privacy> accessed 1 June 2023.

frameworks that bolster, rather than erode, their capacity to exercise their right to unrestricted enjoyment.[186]

The right to privacy is a fundamental human right that is subject to certain qualifications. The entitlement to privacy is expressed in all the significant global and local human rights instruments, encompassing: 'Article 12 of the UDHR in 1948 which stipulates that individuals shall not be subjected to unwarranted interference with their privacy, family, home, or correspondence, nor shall they be subjected to attacks on their reputation or honour. The entitlement to safeguarding against interference or assaults through legal means is a fundamental right held by all individuals. Article 17 of the ICCPR of 1966 pertains to the right to privacy. The fundamental right of individuals to privacy, family, home, and correspondence shall not be infringed upon by arbitrary or unlawful interference.'

Additionally, individuals shall not be subjected to unlawful attacks on their honour or reputation. The entitlement of safeguarding oneself from external interference or assaults is a fundamental right that is bestowed upon every individual under the law. The entitlement to privacy are enshrined in various international human rights instruments: 'the United Nations Convention on Migrant Workers,[187] the UN Convention on the Rights of the Child,[188] the African Charter on the Rights and Welfare of the Child,[189] the African Union Principles on Freedom of Expression (which pertains to the right of access to information),[190] the American Convention on Human Rights,[191] the American Declaration of the Rights and Duties of Man,[192] the Arab Charter on Human Rights,[193] the ASEAN Human Rights Declaration,[194] and the European Convention on Human Rights.'[195] Constitutional provisions pertaining to the safeguarding of privacy are present in more than 130 countries across all geographical regions of the globe.

The safeguarding of personal data is a crucial component of the right to privacy. The entitlement to safeguard personal data can be deduced from the overarching entitlement to privacy. However, certain international and regional instruments additionally specify a more

[186] Ibid.
[187] Article 14.
[188] Article 16.
[189] Article 10.
[190] Article 4.
[191] Article 11.
[192] Article 5.
[193] Article 16 and 21.
[194] Article 21.
[195] Article 8.

explicit entitlement to the protection of personal data. These instruments include: Various international and regional legal instruments have been established to safeguard the privacy of individuals and regulate the cross-border transfer of personal data. These include: 'the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention 108 for the Protection of Individuals Regarding the Automatic Processing of Personal Data, several European Union Directives and its forthcoming Regulation, the European Union Charter of Fundamental Rights, the APEC Privacy Framework 2004, and the Economic Community of West African States' Supplementary Act on data protection from 2010.' Currently, more than one hundred nations have implemented some type of legislation pertaining to privacy and safeguarding of data.

Nevertheless, it is a frequent occurrence that surveillance is executed without taking into consideration these safeguards. Therefore, it should be the objective of the international institutions to prevent the exploitation of legal provisions and loopholes by influential entities like governments and corporations for the purpose of infringing upon individuals' privacy and collection of personal data.

Moreover, in India, the Supreme Court of India acknowledged privacy as a fundamental right under the Indian Constitution in August 2017 by passing the judgement in the Justice K.S. Puttaswamy case,[196] in which a bench of nine judges unanimously, and after due consideration of all personal liberties declared that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms granted by Part III of the Constitution". In India it was K.S. Puttaswamy, a retd. Judge of the Karnataka High Court who played a significant role in the development of the privacy jurisprudence in India. His case[197] in the Supreme Court of the court acknowledge the right to privacy in India and elaborated on the different aspects of the right to privacy.

However, it would be wrong to think that the KS Puttaswamy case was the first case in India which had discussed the right to privacy.[198] The Supreme Court of India developed its jurisprudence of broader rights within the Right to Privacy and has further recognized that the Right to Privacy imbricates itself with many other fundamental rights which is provided in Part III of the Constitution of India, and has several facets to it. Thus, recognizing the right to

[196] *Justice K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1.
[197] Ibid.
[198] Smitha Krishna Prasad et al, 'Privacy and the Indian Supreme Court' National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf> accessed 1 June 2023.

Privacy in relation to several issues such as: 'surveillance, search and seizure, phone tapping by law enforcement authorities, freedom of the press, the right to information, informational privacy, dignity and bodily integrity of women and other vulnerable individuals and groups, and more broadly the autonomy of an individual person.' Hence, the Supreme Court of India has not only upheld these rights but also developed jurisprudence which would be enabling individuals to meaningfully exercise their right associated with privacy and challenge the violations of such rights.[199]

Moreover, in the case of Justice K.S. Puttaswamy,[200] the Supreme Court of India also brought together and elaborated on several aspects of the right to Privacy and examined how the right associated with Privacy has been applied in India since its independence and how it is shaping forward for the future by respecting the Constitutional rights in India. As this discussion was set amidst an era of rapid digitalization in the country initiated by the government of India in order to bring many populations access to the internet through programs like the 'Digital India.' There was a growing uncertainty about how to apply human rights law in the era of technological advancement comprising of the internet and social media. Hence our constitutional history along with international frameworks were being referred to for guidance in order to address these issues. Thus, in the matter of Justice K.S. Puttaswamy,[201] not only the Supreme Court of India's own growing jurisprudence on privacy but also the jurisprudence developed by courts across various nations on privacy along with researches, principles and doctrines developed over the world across a period of over 100 years on Privacy were taken into consideration in order to develop the Right to Privacy as a fundamental right under the Constitution of India. Therefore, the case of 'Justice K.S. Puttaswamy (Retd.)'[202] serves as a fundamental basis for the legal principles surrounding the 'Right to Privacy' in the Indian. This case was adjudicated by a panel of nine judges who unanimously upheld the status of the right to privacy as a fundamental right in Constitution of India. Thus, this verdict of the Supreme Court of India made the entitlement to privacy as a crucial component of the liberties which fundamental rights provided in the Constitution, and facet of autonomy, dignity, and freedom.

Furthermore, the legality of the Aadhaar database was called into question in 2015, when the issue of 'whether the right to privacy constituted a fundamental right was raised?' Replying to this the State's Attorney General contended that the fundamental right to privacy was uncertain

[199] Ibid.
[200] *Justice K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1.
[201] Ibid.
[202] Ibid.

in the Indian Jurisprudence by citing two previous cases: M.P. Sharma case,[203] which was decided by an eight Judge Bench, and the Kharak Singh case,[204] which was decided by a six Judge Bench. In both instances, the State contended that the Constitution did not explicitly safeguard the fundamental right to privacy based on the observations made.

Concurrently, several subsequent legal decisions throughout the years have acknowledged the fundamental nature of the right to privacy. Nevertheless, the rulings that validated the presence of the privacy entitlement were issued by panels with a lesser number of judges compared to M.P. Sharma and Kharak Singh. Thus, the Puttaswamy case was referred to a nine Judge Bench of the Supreme Court due to concerns regarding the precedential value of judgements and recognising the significant significance of the right to privacy. However, in the Puttaswamy case,[205] the Bench reached a unanimous decision that the protection of the right to privacy is an inherent aspect of the right to life and personal liberty provided under Article 21 of the Constitution of India, as well as a component of the freedoms guaranteed by Part III of the Constitution of India. Hence by passing this judgement the Supreme Court of India overturned its previous rulings in the case of M.P. Sharma and Kharak Singh, which had previously held that the Indian Constitution did not recognise the right to privacy. Therefor the case of KS Puttaswamy[206] not only established the right to privacy as a fundamental right, but also emphasised the necessity of enacting a new legislation pertaining to data privacy in India. Thus, broadening scope of protecting people from future tech developments which can breach privacy and data protection such as the Immersive Technology.

Furthermore, the Puttaswamy case[207] also broadened the extent of 'right to privacy' in individual domains and deliberated on privacy as an inherent value. This case was instigated by a plea submitted by Justice K.S. Puttaswamy who was a former judge of the Karnataka High Court, concerning the privacy aspect of the Aadhaar Project which was led by the UIDAI. The UIDAI is an Indian statutory body which issues an unique 12-digit identification number known as the Aadhaar number to its Indian Citizens. The Aadhaar initiative was integrated with multiple social welfare programmes, aimed at optimising the service delivery mechanism and eliminating fraudulent recipients. The legal petition initiated by Justice Puttaswamy aimed

[203] *M.P. Sharma v. Satish Chandra, District Magistrate, Delhi*, (1954) SCR 1077.
[204] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332.
[205] *Justice K.S. Puttaswamy v. Union of India*, (2019) 1 SCC 1.
[206] Ibid.
[207] Ibid.

to contest the constitutionality of the Aadhaar card programme. Subsequently, the Supreme Court was approached with additional petitions contesting various facets of Aadhaar.[208]

In 2015, a three-judge panel of the court was presented with a challenge to the government's collection and aggregation of demographic biometric data, which was alleged to infringe upon the right to privacy of an individual. Thus, the Attorney General of India, presented a legal argument contesting upon the presence of the fundamental right to privacy, drawing upon the rulings in M.P. Sharma and Kharak Singh. While addressing the challenges, the three-member panel of judges duly acknowledged various rulings of the Supreme Court of India wherein the constitutional safeguarding of the fundamental right to privacy was upheld. Nevertheless, the rulings that upheld the presence of a constitutionally safeguarded privacy right were issued by panels with a lesser number of judges compared to the ones in M.P. Sharma and Kharak Singh. Hence, the matter was directed to a Constitution Bench for the purpose of examining the precedents established in M.P. Sharma and Kharak Singh, as well as the accuracy of subsequent rulings.

On the 18th of July in 2017, a Constitution Bench finally deemed it fitting for the matter to be resolved by a bench of nine judges.[209] With the issue 'whether the right to privacy was a fundamental right under Part III of the Constitution of India?' The Respondents who were the subject of this legal matter primarily drew upon the rulings in the M.P. Sharma and Kharak Singh cases, which had previously noted that the Constitution of India did not explicitly safeguard the entitlement to privacy. The pronouncements were made by a panel of eight and six judges, respectively. The respondents contended that these pronouncements would hold precedence over subsequent judgements rendered by smaller panels. The Respondents contended that the framers of the Constitution did not have the intention of establishing the right to privacy as a fundamental right under the Constitution of India. Conversely, it was contended by the Petitioners side that the rationales presented by the case of M.P. Sharma and Kharak Singh were based on the principles laid in the A.K. Gopalan case.[210]

The Petitioners contended that the ruling in the case A.K. Gopalan, interpreted each provision within the Chapter on fundamental rights in the Constitution of India as representing a separate safeguard, was deemed invalid by an eleven Judge Bench in the case Rustom Cavasji

[208] Smitha Krishna Prasad et al, 'Privacy and the Indian Supreme Court' National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf> accessed 1 June 2023.
[209] Ibid.
[210] *A.K. Gopalan v. State of Madras*, (1950) SCR 88.

Cooper.[211] Thus, the Petitioners side contended that the foundation of the preceding rulings lacked validity and it has been suggested that the seven Judge Bench ruling in the Maneka Gandhi case[212] endorsed the dissenting opinion of Justice Subba Rao in the case of Kharak Singh, while invalidating the majority decision.

Furthermore, additional arguments presented in the hearing pertained to the extent of the privacy right. The Petitioners advocated for a comprehensive framework of privacy as an essential entitlement, encompassing various dimensions. Conversely, the Respondents contended that privacy was an equivocal notion, and its recognition could only be achieved through the establishment of legal provisions and judicial precedents. The Petitioners contended that a harmonious interpretation of the Constitution must be adopted in consonance with the Preamble, while bearing in mind the intrinsic nature of privacy as a fundamental right and a universally recognized human right. The respondents espoused a limited perspective that centred on the Constitution as the primary source of fundamental rights and vested the authority to amend them solely in the Parliament. The Supreme Court of India has established, through six distinct opinions, that privacy is a fundamental right that is separate and independent under Article 21 of the Constitution. The essence of the ruling delineated a broad construal of the entitlement to privacy. It did not constitute a limited entitlement against mere physical intrusion, nor a secondary entitlement under Article 21, but rather one that encompassed both the physical and mental aspects of an individual, comprising decisions, preferences, data, and autonomy. The Constitution's Part III was deemed to recognize privacy as a fundamental right that is comprehensive in nature and can be enforced through various means. The various opinions delved into the specifics of the extent of the right. The Court has overturned the verdicts in M.P. Sharma and Kharak Singh, to the extent that the latter decision had determined that the right to privacy did not qualify as a fundamental right.

Regarding M.P. Sharma, the Court determined that the ruling was legitimate in affirming that the Indian Constitution did not incorporate any constraints on search and seizure laws that were comparable to the Fourth Amendment in the Constitution of the United States. The Court determined that while the Fourth Amendment did not provide an all-encompassing definition of privacy, the lack of a similar safeguard in the Constitution did not necessarily signify a complete absence of an inherent right to privacy in India. Consequently, the decision in M.P. Sharma was overturned. The Court dismissed the notion of personal liberty as an insular

[211] *Rustom Cavasji Cooper v. Union of India*, (1970) 1 SCC 248.
[212] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

concept, commonly known as "ordered liberty" as espoused by Kharak Singh. Justice D.Y. Chandrachud referred to this approach as the "silos" perspective, which was derived from the case of A.K. Gopalan.

The Court noted that the practice of compartmentalizing fundamental rights was abolished after the Maneka Gandhi case.[213] The Court noted that the majority decision in Kharak Singh contained an inherent inconsistency, as the legal justification for invalidating domiciliary visits and police surveillance could only be based on the right to privacy, which was acknowledged in principle but deemed to be outside the purview of the Constitution.

The Court has further determined that subsequent decisions affirming the right to privacy following Kharak Singh are to be interpreted in accordance with the principles established in the ruling. The Court conducted an analysis of the affirmative case to determine whether the right to privacy was safeguarded under the right to life, personal liberty, and the freedoms guaranteed under Part III of the Constitution. The court ruling concluded that privacy is not a concept exclusive to the elite. The argument posited by the Attorney General, which suggests that the relinquishment of the right to privacy is necessary for the provision of state welfare entitlements, was dismissed. The judgement held that although the right to privacy is not absolute, it is of great importance. Additionally, it provided an outline of the appropriate standard of judicial review that should be employed in instances where the State encroaches upon an individual's privacy. According to this principle, limitations on the right to privacy may be imposed if the infringement satisfies the three criteria. The three fundamental principles that govern the justification of state action are legality, need, and proportionality. Legality presupposes the presence of a legal framework, while need is determined by a legitimate state objective. Proportionality, on the other hand, guarantees a logical connection between the ends and the means employed to achieve them. Justice S.K Kaul introduced an additional criterion to this assessment, which required "procedural safeguards against the misuse of such intervention." Simultaneously, Justice J. Chelameswar asserted that the criterion of "compelling state interest" ought to be exclusively employed in privacy assertions that warrant "strict scrutiny." Regarding additional assertions related to privacy, he maintained that the standard of justice, fairness, and reasonableness as stipulated in Article 21 would be applicable. The determination of whether the "compelling state interest" standard is applicable would be contingent upon the specific circumstances of the case, as per his assessment.

[213] (1978) 1 SCC 248.

The Court underscored the significance of sexual orientation as a fundamental aspect of privacy. The text delved into the positive and negative aspects of the right to privacy, highlighting that the State is not only prohibited from infringing upon this right but also has a duty to implement appropriate measures to safeguard an individual's privacy. The ruling established that the right to informational privacy is encompassed within the broader right to privacy. The Court acknowledged the necessity of a legislation pertaining to data protection; however, it deferred the responsibility of enacting such a law to the Parliament.[214]

3.2. DATA PROTECTION AND ITS PRINCIPLES

In the contemporary society, it is commonplace for all individuals within the digital ecosystem to possess an electronic mail address. A significant number of individuals possess electronic mail accounts on costless internet-based electronic mail platforms. A standard Gmail account provides a storage capacity of approximately 15 GB for user data retention. The electronic mails stored in a G-mail account generally constitute an individual's data, which may relate to their personal or occupational affairs. Likewise, one's Facebook account serves as a manifestation of their cognitive expressions, primarily in the form of posts, which can be classified as data. We are currently residing in the contemporary era. Our presence is crucial within the digital and mobile ecosystems. In the past two decades, there has been a rapid advancement in technology that has significantly transformed our daily routines. There is a growing dependence on digital data and a consistent rise in the generation of mobile data. In contemporary times, individuals possess the ability to function as worldwide authors, publishers, and broadcasters of digital information within the realm of technology. The magnitude of data has significantly increased over the past twenty years. The volume of data transmitted over the Internet, commonly referred to as internet traffic, and has experienced a notable surge. Internet traffic can be categorized into two types: fixed internet traffic and mobile internet traffic. The term “Fixed Internet Traffic” may pertain to the data transmitted by residential and commercial subscribers to their respective ISPs, cable companies, and other similar service providers. The term “Mobile Internet Traffic” may pertain to the backhaul traffic that is transmitted from cellular towers and service providers. According to Cisco's projection, the quantity of network-connected devices is anticipated to surpass 15 billion,

[214] Smitha Krishna Prasad et al, ‘Privacy and the Indian Supreme Court’ National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf> accessed 1 June 2023.

which is twice the global population, by the year 2015.[215] As per the fifth edition of the Cisco VNI Forecast spanning from 2010 to 2015, it has been projected that the overall worldwide Internet traffic will experience a fourfold increase and attain a yearly volume of 966 exabytes. According to projections, the monthly global consumer IP traffic is anticipated to attain 107,985 petabytes in 2018, with a compound annual growth rate of 21%. Consumer traffic comprises of stationary IP traffic that is produced by households, university communities, and Internet cafes. According to the "Handset Data Traffic (2001-2017)" forecast by Strategy Analytics, there is a projected significant increase in the advancement of mobile phones. Moreover, it has been asserted that the quantity of traffic data will increase from 5 exabytes annually to more than 21 exabytes per year by 2017.[216] According to data from internetworldstats.com, the number of internet users in India increased from 5,000,000 in the year 2000 to 462,124,989 by 2016.[217] Subsequently, the statistic has experienced a significant surge, primarily attributed to the substantial expansion of the mobile web industry in India. Therefore, data has become increasingly significant in our daily lives. Undoubtedly, there is an incessant generation of electronic data concerning individuals, emanating from diverse sources such as computer systems, communication devices, computer resources, and other digital devices. The result has been a significant increase in the quantity of data produced daily, necessitating the implementation of measures to safeguard it.[218]

The act of producing, disseminating, and transmitting data on a worldwide scale underscores the critical importance of safeguarding data through the implementation of robust data protection measures. The internet is a highly impactful innovation in human history, following the introduction of fire. The Internet has had an unparalleled impact on the development of humanity, surpassing any other singular event. The emergence of the internet has had a dual effect, rendering geography obsolete while simultaneously introducing the data economy. As a result, information stored on a specific website in each country can be accessed globally with ease through a simple click of a computer mouse. Given the circumstances, it is reasonable to anticipate that safeguarding and conserving this information would become a crucial concern

[215] ITP Staff, 'Cisco predicts 15b connected devices by 2015' (*edge*, 14 June 2011) <https://www.itp.net/news/585110-cisco-predicts-15b-connected-devices-by-2015> accessed 2 June 2023.
[216] Nitesh Patel, 'Handset Data Traffic' (Strategy Analytics, 18 June 2012) <https://www.strategyanalytics.com/access-services/media-and-services/mobile/wireless-media/wireless-media/reports/report-detail/handset-data-traffic-(2001-2017)> accessed 2 June 2023.
[217] 'India Internet Usage Stats and Telecommunications Market Report' (Inter World Stats, 2016) <https://www.internetworldstats.com/asia/in.htm> accessed 2 June 2023.
[218] Pavan Duggal, *Data Protection Law in India* (Universal Law Publishing, 2016).

not only for individuals and organizations, but also for nations themselves. As a result, the notion of safeguarding data has become prevalent globally.[219]

At this point, let us analyse the concept of data protection. Various sources and legal entities have provided varying definitions and interpretations of data protection. As per the definition provided by Collinsdictionary.com, the term "data protection" pertains to measures implemented to ensure the protection of personal data stored on a computer. According to Dataprotection.eu, the term data protection refers to a form of privacy protection that is characterized by specific legal regulations. The right to data protection guarantees an individual the authority to control all data pertaining to their personal identity. The Constitutional Court of Hungary has expounded upon the concept of data protection as it pertains to the right to informational self-determination. This right refers to an individual's fundamental authority to make decisions regarding the disclosure and utilization of their personal data. Therefore, the term Data Protection can be characterized as the intricate interplay between the acquisition and distribution of data, technological advancements, societal norms regarding privacy, and the legal and political implications that arise from these factors. It can be argued that the notion of Data protection pertains to safeguarding the individual, i.e., the human entity, and specifically, the protection of the data subject rather than the data itself.[220]

The concept of data protection has a long-standing history. Since their inception, civilizations have prioritized safeguarding and maintaining their data. Various civilizations have implemented diverse methods to safeguard data, which can be attributed to this rationale. Throughout human civilization, the protection of data has been a paramount concern. This is evidenced by the implementation of rudimentary mechanisms for safeguarding information in ancient societies. The ancient Indus Valley Civilization employed inscriptions as a means of safeguarding their data. The preservation of additional significant information was also achieved using seals. Indeed, certain seals were utilized for the purpose of impressing clay on commercial commodities, although they served additional functions as well. Throughout history, various monarchs and empires have endeavored to safeguard information by preserving it in diverse tangible formats, such as stone. The emergence of the printing press facilitated a significant upsurge in the expansion of literature and presented an additional avenue for safeguarding information, as data was transcribed onto paper. The emergence of the modern era has brought forth a plethora of digital and electronic data, highlighting the necessity

[219] Ibid.
[220] Ibid.

for safeguarding and conserving such information. The data in question manifests in four distinct formats: audio, video, image, and text, which are currently recognized by contemporary society. The emergence of computers represented a significant advancement in safeguarding and conserving data, as they offered an additional means of data protection. The advent of the Internet and the subsequent worldwide proliferation of data have compelled various nations to establish unique national regulations to address data protection. In addition, numerous international organizations have been engaged in formulating principles related to safeguarding data. From a layperson's viewpoint, data protection pertains to the appropriate handling of personal information of individuals. The concept of data protection establishes specific standards and regulations for safeguarding data and its inherent authenticity. The regulations in question pertain to the acquisition and utilization of data, the caliber and safeguarding of data, and the entitlements of persons in relation to data concerning their own selves. The primary objective of data protection is safeguarding the entitlements of individuals in relation to their personal information. The implementation of data protection measures yields advantageous outcomes in the handling of information and does not impede efficient business operations in both public and private domains, if it is appropriately executed.[221]

Hence let us try to investigate the development of data protection principles across different regions of the globe in order to understanding the regulations which is protecting the important data in the internet.

Data Protection Directive 95/46/EC of the European Union represents significant advancement in the realm of data protection. Several significant principles have been established, including: Data Protection Directive Principles, principles on collective limitation, purpose specification, individual participation, data quality, security safeguards, openness, use limitation, and accountability. Moreover, the privacy framework of the APEC has aimed to prioritize the identification of actual or potential harm arising from the disclosure of information, rather than emphasizing the individual's rights concerning their information. The AICPA and the CICA have jointly developed the GAPP. The practices are derived from globally recognized fair information principles that are incorporated in numerous privacy laws and regulations across different jurisdictions. These practices are also acknowledged as sound privacy measures. In addition to the global endeavors concerning data protection, numerous nations have developed their own domestic regulations to address this matter.

[221] Ibid.

In United Kingdom's Data Protection Act of 1998, Schedule 1 enumerates the principles of data protection. It is evident that the individual's data processing should adhere to principles of fairness and lawfulness. According to Schedule 2 of the Act, there are six conditions that must be met for data to be considered "fairly processed." At least one of these conditions must apply to the data in question.

The inclusion of location information as CPNI was a notable feature of the 1996 Telecommunications Act in the USA. This information was added to the existing data points of time, date, duration of a call, and the dialed number. The E911 Act or WCPSA of 1999, addressed the oversight by mandating the opt-in provision for location data employed for all non-emergency objectives. The ECPA of 1986 has been construed to encompass the surveillance of electronic correspondences, as well as oral and wire communications within the confines of the workplace and precludes their deliberate interception and divulgence. As per the ECPA, interception refers to the procurement of the substance of an electronic communication by means of any electronic, mechanical, or other apparatus. The provision has been construed to proscribe the act of listening to, perusing, or duplicating electronic communications during their transmission to their ultimate endpoint, unless there exists an exemption under the relevant legislation. The act of capturing oral, wire, or electronic communications during any stage of transmission using monitoring devices or software would be classified as interception, as per the definition provided under Title I. The exception of prior consent for intercepting a communication remains applicable irrespective of whether the interception was conducted in the regular course of business. According to Section 2511(2) (d) of the ECPA, the interception of a communication does not constitute a violation of Title I if the individual conducting the interception is a participant in the communication or if one of the participants has previously given consent to the interception. However, it should be noted that intercepting a communication for the purpose of committing a criminal or tortious act is still considered a violation. Title II of the ECPA pertains to stored communications and establishes legal responsibility for individuals or entities that obtain access to stored communications without proper authorization, or surpass the authorization granted to obtain information from a facility that provides electronic communication services. The ECPA of 1986 contains pertinent clauses pertaining to this matter as follows: S 2511, S 2515, S 2516, S 2517, and S 2701. Thus, the ECPA has enabled the US to implement a tailored strategy in the realm of safeguarding and preserving data privacy.

The Australian Privacy Act of 1988 delineates a series of principles concerning information privacy that pertain to the subject of data protection. The Information Privacy Principles are delineated under Section 14. The Information Privacy Principles encompass guidelines on collection, solicitation, and storage of personal information; Information, access, and alteration of records; Usage, limits, and disclosure of personal information, among other things. Moreover, S 15 of the Australia's Privacy Act, 1988 talks about the 'application of information privacy principles stating that certain principles like 1, 2, 3, 10 and 11 applies after the commencement of this Act' and principles 4 to 9 apply to information records in the possession of an agency, regardless of whether the information was collected before or after the commencement of this Act.' Moreover, Section 16 of the act stipulates that it is impermissible for an agency to refrain from acting or to partake in any conduct that violates any of the Information Privacy Principles. Furthermore, the Telecommunication and Interception Act of Australia has undergone a thorough review and revision process to ensure the safeguarding of individual privacy. Section 108 of the 2006 Telecommunication and Interception Amended Act pertains to the prohibition of accessing stored communications. Nevertheless, stored communication may be accessible to individuals with warrants and authorized inspectors. Upon reviewing the provisions, it can be inferred that while an individual's personal information is recorded and maintained by a designated record keeper, it is subject to verification prior to usage. Additionally, the record keeper bears the responsibility of ensuring that the personal information is not tampered with or exploited in any manner. Australia has developed a distinct approach to address the matter of safeguarding data.

China functions as the primary nucleus of the mobile industry. The country in question exhibits the highest rate of mobile phone penetration on a global scale. A diverse range of mobile phones can be procured at reasonable prices. Within this context, it is of utmost importance to conduct an analysis of the data protection laws in China.

In accordance with the provisions outlined in Article 6 of the China Telecommunication Act, any interception or recording of communications that are transmitted through telecommunications companies or dedicated telecommunications channels is strictly prohibited in the absence of appropriate authorization. Furthermore, any infringement upon privacy through illegitimate methods is illegal. Ensuring the confidentiality of processed communications is a crucial and necessary undertaking for telecommunications organizations. In accordance with Article 7, it is admissible for any telecommunications corporation to provide the relevant communication records upon necessary fees payment to subscriber who

asks for their own communication records. As per the provisions of Article 8, the onus lies on the telecommunications user to assume responsibility for the substance of their telecommunications, along with any consequent ramifications or sway. If a telecommunications enterprise concludes that a user's business operations, which involve the delivery of telecommunications content, are harmful to public order and ethical standards, the enterprise may opt to terminate the user's access to telecommunications services. As per the provisions of Article 9, the use of telecommunications by an individual who lacks legal capacity or has limited legal capacity shall be deemed as an act carried out by an individual possessing legal capacity. It is noteworthy to observe that China has implemented regulations concerning mobile telecommunication services, indicating significant progress in this domain. Initially, the term "Mobile Telecommunications" is defined as the transmission of voice or data via wireless communication networks utilizing radio terminal equipment. In accordance with Article 35, it is required that mobile communication systems and their associated monitoring facilities adhere to the Communication Protection and Supervision Act and its corresponding regulations. As per the provisions of Article 40, the carrier is obligated to adhere to the ensuing regulations: i) The connection established must not infringe upon the privacy of other individuals; ii) The telecommunication service provided must maintain an appropriate level of quality; iii) The connection established must not result in any harm to the facilities belonging to users or other public communication networks.

China has endeavored to address the matter of safeguarding data, considering its significant populace and the proliferation of mobile technology. Therefore, it can be asserted that various nations have implemented diverse approaches and systems to address the significant matter of data privacy. Numerous countries worldwide have adopted the perspective that safeguarding national security is of utmost importance, and that the safeguarding and maintenance of national security, integrity, and sovereignty supersedes that of data protection and privacy in the event of a clash between the two. The contemporary era is characterized by a transformative interregnum. The advancement of technologies necessitates a corresponding evolution of the principles of safeguarding data and ensuring privacy, particularly considering the emergence of the knowledge economy and the information society.

India has abstained from endorsing any global framework pertaining to data protection. Data protection has not been given priority in the national legislation. At present, India lacks a dedicated legal framework for the protection of data. Despite the implementation of several substantial data protection legislations by different nations, including the United Kingdom and

the European Union, this matter remains unresolved. Upon conducting a more thorough analysis of the issue pertaining to data protection, it is evident that several legal regulations in India exert a substantial impact on the preservation and protection of data and information. Contemporary data protection laws prioritize the safeguarding and conservation of electronic data, as evidenced by current legislative trends. Therefore, it is pertinent to investigate the legal provisions in India concerning the safeguarding and conservation of data and information in electronic format. India has enacted specific legislation pertaining to electronic data and information. The Indian Information Technology Act of 2000 underwent modification through the Information Technology (Amendment) Act of 2008. The Information Technology Act of 2000, commonly referred to as the Indian Cyber law, encompasses several provisions that significantly influence the safeguarding and conservation of electronic data and information. But, in order to protect Data in India, India needs to step up and make a separate specific law on Data Protection in accordance with the principles just discussed above in order to address the pressing issues related to Data Protection in India such as the collection of Biometric Details in Aadhar, collection of data from mobiles, browsing history, surveillance capitalism by foreign and domestic tech companies of India. Considering these challenges and the Facebook-Cambridge Analytica Scandal, its high time that India should also finally make a Data Protection Act considering all these issues into consideration.[222]

3.3. DISCUSSION ON PRIVACY & DATA PROTECTION IN AR/VR

3.3.1. INTRODUCTION

In the above section of this chapter, the researcher has discussed about issues of Privacy and Data Protection and the relevant laws specifically International Human Rights Laws which deals with such issues. Furthermore, the researcher in the above section also discussed some of the case laws from the country India in order to explain the value and necessity of Privacy and Data Protection in Human Rights Law. Thus, establishing the fact that how important is Right to Privacy and Data Protection as human right. In the present section, let us discuss about the Privacy & Data Protection under AR/VR.

The utilization of AR/VR devices poses unique challenges to safeguarding user privacy, primarily due to the extensive range, magnitude, and confidentiality of the data they gather. In order to address potential negative consequences, it is recommended that policymakers

[222] Ibid.

undertake a reform of the current regulatory framework for data privacy, which is characterized by a fragmented approach that overlooks certain risks while excessively regulating others.

In a contemporary society that is progressively reliant on digital technology, the adage "your reputation precedes you" may or may not retain its validity. Nevertheless, some form of data pertaining to an individual is typically available. The utilization of user data facilitates the creation of dynamic and personalized experiences across a range of technological platforms, including digital communication channels and smart devices. In the absence of adequate measures to ensure data protection, the extensive acquisition and manipulation of personal information, particularly by entities with lax or unethical practices, may subject individuals to potential privacy hazards. The ecosystem of technology is witnessing a burgeoning presence of devices and applications that facilitate augmented reality or virtual reality. These immersive technologies empower its users to encounter digitally created content in both physical and virtual realms.

The realm of AR and VR encompasses a variety of technological applications, such as those found on mobile devices which integrate images with digital components. There are HMDs that superimpose digital elements onto a user's physical surroundings, as well as headsets that facilitate navigation within entirely virtual environments. Immersive technologies and applications collect considerable quantities of personal data which comprises of data furnished, generated and data deduced about users of such immersive technologies in order to provide the users with such ethereal experiences.

The employment of augmented reality or virtual reality technology presents new privacy concerns for three distinct reasons: (i) The Augmented Reality and Virtual Reality devices comprise various information-gathering methods through its technology with each of these technologies posing distinct risks of privacy and approaches of mitigation; (ii) AR/VR devices are known to collect a significant amount of sensitive data, which is not typically gathered by other modern day tech devices; and (iii) this extensive information gathering process is essential for the fundamental operations of immersive technologies.[223]

AR/VR technologies can be deconstructed as an assemblage of sensors and displays that collaborate to generate a virtual encounter for the users of such technology. In order to simulate virtual elements within a 3D tangible space or even entirely digital worlds such as the

[223] 'The XRSI Privacy Framework version 1.0' (*XRSI,* September 2020) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 2 June 2023.

Metaverse, these technologies necessitate some fundamental user-provided data as a foundation for its functioning which is followed by a continuous generation of new data by users while engaging in activities inside the virtual surroundings. The feedback information, both initial and continuous, may encompass biographical and demographic particulars, location, and mobility data, as well as biometric data. AR/VR devices and applications are increasingly incorporating advanced functions, such as gaze-tracking and interpreting neural signals by BCI technologies, which have led to the emergence of new techniques of consumer data collection. The data streams generated by AR/VR devices may potentially encompass various types of personal, identifiable, or confidential information. Furthermore, these devices may amalgamate such information, thereby uncovering or deducing supplementary particulars about individual users.

The distinctive features of AR/VR technologies, as compared to other consumer devices and applications, are attributed to the extensive and comprehensive user data collection required for their fundamental operations. Notwithstanding, the categories of data gathered, the hazards to privacy, and the likelihood of immediate detriments in the absence of protective measures are analogous to those of other internet-based technologies and interconnected apparatuses, a significant number of which have already been extensively embraced by consumers. The employment of immersive technologies poses distinctive challenges, primarily stemming from the potential hazards of consolidating confidential data and the difficulty of implementing counteractive initiatives which were originally formulated for other modern-day technologies within a 3D virtual setting.

The diverse array of data collected by AR/VR devices necessitates nuanced policies. Treating AR/VR as a singular entity risks excessive regulation of select data collection practices, while simultaneously failing to adequately safeguard other forms of data. Simultaneously, the regulation of individual technologies employed to provide immersive experiences will result in policy lagging innovation, given the constant emergence of new capabilities and user cases. Rather than the current approach, policymakers need to tackle concerns of privacy inside the virtual world by considering the various categories of data which devices of immersive technologies gather and by implementing measures required for safeguarding users against any potential harm that may result from such data collection. The objective is to establish a regulatory framework that is all-encompassing and impartial towards technology, thereby providing ample space for companies engaged in the development of AR/VR devices to persist in their innovative pursuits, while simultaneously minimizing potential negative consequences.

It is imperative that pertinent federal regulatory entities in the USA furnish direction and elucidation regarding the application of extant legislation, such as the HIPAA and the COPPA, to AR/VR devices and applications. The reform of privacy laws, including COPPA and HIPAA, by Congress in the USA is recommended to prevent unnecessary limitations on the use of AR/VR technologies in specific sectors or by certain users. The Congress (US) and relevant rulemaking bodies should establish regulations that promote transparency and choice to safeguard against potential adverse impacts from newer data collection technologies. For example, 'biometric identification' and 'personal information inferred from biometric data.' It is suggested that federal privacy legislation be enacted by lawmakers to ensure compliance requirements are harmonized at the national level, rather than relying on regulations that are implemented by states. Additionally, government agencies and industry should collaborate to bring user control (for example, opt-out mechanism) and security guidelines for such virtual and augmented reality developers and transparency and disclosure practice as well to counter the new risks presented by data sourced from biometrics.[224]

This section of the paper aims to provide a comprehensive overview of the collection of user data in the context of AR/VR technologies, within the framework of acquisition of information and protection of privacy within such immersive technologies. Specifically, this section outlines four distinct categories of personal data that are collected by AR/VR technologies, namely observable, observed, computed, and associated data. Furthermore, this section examines the data collection practices employed by AR/VR technologies falling within these categories, and highlights the privacy concerns that arise as a result of such data collection. Furthermore, in this section the researcher examines the established measures for mitigating risks associated with various types of personal data and analyze the unique challenges that arise in protecting user privacy when using immersive technologies, which go beyond those encountered in traditional digital technologies. These challenges include the criticality of biometric data, the insufficiency of current mitigation strategies, and the potential for increased harm to vulnerable users. Lastly, the researcher examines the existing regulatory framework concerning user privacy, specifically exploring the pertinent statutes and guidelines that pertain to AR and VR. This analysis will identify policy domains that necessitate further consideration

[224] Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation*, March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 2 June 2023.

and culminate in suggestions to address the novel challenges put forth by AR/VR technologies on an user's privacy and data.

3.3.2. DISCUSSION ON COLLECTION OF USER INFORMATION IN AR/VR

The optimal user experience and unique functionalities of AR/VR devices are contingent upon the integration of information from various sources. In the realm of virtual space and other such technologies which collect information's, the collection of information of the users of such technology can be classified into four distinct categories of data: Observable Data, Observed Data, Computed Data and Associated Data. The 'observable data' refers to the information pertaining to an individual that can be observed and replicated by AR/VR technologies and other third parties. It includes the digital media which is produced by an individual or by their digital interactions within the digital world. The 'observed data' refers to information that is disclosed or produced by an individual and can be perceived by external parties, but cannot be reproduced by them. Examples of such information include biographical details and location data. The 'computed data' refers to AR/VR technologies which derives its new insights by analyzing both observable and observed data, including biometric information such as identity and advertising profiles. And the 'associated data' refers to data that lacks descriptive information about the user of such technology. For example, a username or IP address.[225]

In some cases, it is observed that in complex technologies like AR/VR, the specific data may have the potential to contribute to different types of data based on the way they are gathered and analyzed. For example, an illustration of basic health and fitness measurements like heart rate are considered observed data, and related computed information like estimated calories spend during physical activity is regarded as Computed data.

Diverse data categories have a crucial role in the building of immersive and interactive virtual environments and entities, each with distinct implications for privacy. Consequently, it is imperative to establish optimal guidelines to address novel and intensified privacy issues.[226]

[225] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* October 27, 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 2 June 2023.

[226]Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 2 June 2023.

As discussed previously there are four different types of user information collection data. Let us have a closer look on these four different types of user information collected during the usage of immersive technologies.

3.3.2.1. OBSERVABLE DATA

Certain data can be perceived reliably and objectively by external parties. Based on the observable data, it is possible for other individuals to directly perceive the same information about the user. In the context of digital privacy, potential areas of concern may encompass private communication, user-generated media, or media content captured by third-party entities. AR/VR technologies utilize observable data to facilitate the creation of a virtual presence, either within entirely virtual environments generated by VR or within tangible environments augmented with virtual components via AR.[227]

The virtual representation of oneself, commonly known as an avatar, can be classified as personally Observable information, especially if the avatar is a highly realistic depiction. Avatars that are less realistic, but created by users to represent their physical or outer appearance, can still convey certain demographic characteristics, like gender and race. In contrast to static 2D depictions, like display pictures or digital photographs, 3D avatars utilized in totally immersive Virtual Reality encounters serve as a programmed manifestation of an user which primarily comprises of their physical attributes, gestures, and behavioural tendencies.[228] Individuals perceive these digital avatars in a manner akin to their physical bodies, thereby rendering this specific type of data more personal than analogous 2D data.[229] Apart from the virtual depictions of the user's corporeal identity, AR/VR gadgets also gather specific observable information regarding their social engagements and associations within the virtual realm in VR or the application realm in AR. Like other technological advancements, specific modes of communication, such as instant messaging, can be considered as empirical information. AR/VR can capture observable data in the digital formats like video, images, or screenshots which depicts an individual engaged in specific activities. This data can be collected for various purposes, such as redistributing event recordings or for more nefarious

[227] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation, 27 October 2017*) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 2 June 2023.
[228] Fiachra O'Brolcháin et al, 'The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy' (2016) Science and Engineering Ethics 22 <https://doiorg/10.1007/s11948-014-9621-1> accessed 2 June 2023.
[229] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 2 June 2023.

reasons, such as taking pictures of individuals within the private spaces without their personal consent. Moreover, due to their complete virtual nature, a user's presence and interactions can be regarded as observable data as they are processed and rendered. This may encompass audio or video captures of virtual interactions within AR/VR platforms or applications, produced by both commercial entities and non-affiliated users. The acquisition of observable data is a crucial prerequisite for the development of interactive experiences in the realm of AR and VR. This is because the creation of immersive experiences necessitates the simulation of a virtual presence. Although single-user applications, such as individual productivity applications or single-player games, may not necessitate the creation of virtual avatars, the complete collaborative and interactive potential of these technologies is captured by multiuser applications, which do require them. In the absence of these digital depictions, the potential for other users to engage in a completely immersive encounter would be limited.[230]

Insufficient limitation or security measures for such data can pose significant privacy risks for users. Most privacy apprehensions related to observable data pertain to anonymity and personal autonomy. This refers to the capacity of individuals to regulate the extent to which others can identify and monitor them.[231] The determination of the appropriate boundaries for the privacy of observable data is predominantly subjective and heavily dependent on contextual factors. Certain users may opt to grant third-party entities access to a substantial quantity of data, whereas others may elect to disclose solely the essential data required for utilizing a service and engaging with fellow users.

Likewise, individuals may experience a sense of ease in disclosing discernible data to specific cohorts (such as intimate companions or confidants) while opting to maintain confidentiality from other parties (such as employers or business associates). Distinguishing between privacy preferences and factual privacy hazards pertaining to observable data is a crucial undertaking. The disclosure of private or harmful information may occur when a third party collects, records, distributes, or replicates data, resulting in potential privacy hazards. The non-consensual disclosure of sensitive information, such as intimate or private photographs or recordings of an individual, can result in significant personal and reputational harm because observable data can

[230]Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* 4 March 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 2 June 2023.

[231] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* 27 October 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 2 June 2023.

be accessed by multiple users in a first-hand manner. The act of disseminating images or recordings that disclose the identity of an individual in a sensitive setting/location, such as a confidential support group/medical facility, and can potentially divulge personal information which was intended to be kept within a restricted circle. The utilization of observable data has the potential to result in personal-autonomy detriments, particularly when it is employed to imitate an individual or alter their visual representation. An individual with malicious intent has the capability to utilize the image of another person to assume their identity on various communication platforms. In the context of immersive environments, it is possible for an unauthorized individual to utilize other individual's likings to construct a completely interactive avatar. Such an Impersonation can result in harm of reputation and images of an individual by the creation of a false impression that individual participated in activities or interactions that they did not actually engage in.

Furthermore, it has the potential to facilitate fraudulent activities and identity theft, thereby putting individuals at risk of experiencing financial damages. The potential ramifications for privacy arising from the presence of observable data within 2D digital media are similarly present within the immersive realms of AR and VR. The disclosure of information can vary in sensitivity based on observable avatars, social activities, and in-world assets. The levels of user comfort and preferences regarding observable information are subject to variation. In the context of AR/VR, it is observed that certain users may opt for avatars that mirror their physical attributes, whereas others may choose avatars that conceal their appearance or identity. The risk is especially pertinent for individuals who are considered vulnerable, including minors, individuals who utilize AR/VR technology for medical or health-related reasons, and people who disclose important information while engaged in immersive experiences.[232]

The mitigation strategies aimed at addressing privacy risks associated with observable data primarily center on empowering users to exercise control over the viewing and sharing of their data, safeguarding such data against unauthorized access, and instituting legal frameworks that safeguard against the inappropriate use or involuntary dissemination of observable data. AR/VR technologies and their associated applications have the potential to reduce risks by affording user's transparency and control over the collection, sharing, and utilization of

[232]Ellysse Dick, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation*, 4 March 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 20 May 2023.

observable data. Individuals'' privacy preferences vary, and therefore, they can utilize privacy settings to limit third-party access to data that they deem sensitive or private.

As an illustration, individuals may opt to designate the specific users who are authorized to access their photographs or other forms of multimedia. Within the context of AR and VR, it may be necessary to limit users' access to virtual resources and prevent third-party entities from monitoring, eavesdropping, or recording social interactions that occur within the application or virtual environment. Digital communications can be safeguarded by technical measures to protect the information that is observable. The implementation of end-to-end encryption in messaging systems guarantees that solely. The intended recipients possess the ability to access written communications or shared media. However, it is important to note that this measure does not preclude the possibility of recipients sharing the contents of the message with others.

The implementation of technical constraints can potentially impede unauthorized acquisition of user data by external entities without explicit user consent or awareness, for instance, via screenshot capture. However, it is important to note that such technical measures may have certain limitations. In certain instances, such as with a social media platform catering to a susceptible demographic like children or a dating app, it may be advantageous to implement measures that prohibit the capturing of screenshots of user profiles, posts, or private messages. It should be noted, however, that these measures may not be entirely effective in preventing individuals from taking photographs of said content as it appears on their personal mobile devices. Comparable measures can be instituted in AR/VR applications. Although these measures do not provide complete security for the information, they do create additional obstacles for practices that could potentially violate privacy.[233]

Ultimately, the implementation of legal frameworks and regulatory measures can serve as a means of mitigating the malevolent exploitation of publicly available data. There exist several legal statutes in the countries such as United States of America that forbid the exploitation of an individual's perceivable data for malevolent intentions or the acquisition and dissemination of such data without their awareness. The legal framework governing the use of surveillance and recording technologies encompasses a variety of regulations applicable to governmental entities, law enforcement agencies, businesses, and individuals alike. Additionally, there exist legal provisions that prohibit the dissemination of private photographs or recordings. Moreover, District of Columbia and Guam in its 46 states made laws on 'revenge porn'

[233]Ibid.

(nonconsensual pornography) from February 2021 according to the records of the Cyber Civil Rights Initiatives.[234]

3.3.2.2. OBSERVED DATA

Similar to observable information, observed data refers to information pertaining to the user that is either provided or generated by them which are descriptive in nature. In contrast to observable data, the information in question cannot be reproduced by an external entity through observation.[235] The aforementioned information may encompass fundamental biographical details, individual preferences and behavioural patterns, associations and identity characteristics, geographical location or other metadata, and other data which is provided/generated by the user. Empirical evidence is frequently employed to influence a user's interaction with a digital artefact. The significance of this information is particularly pronounced in the context of AR/VR products and services, as they largely depend on it to offer a completely immersive experience to the end-user.

A considerable proportion of data pertaining to AR/VR belongs to this classification owing to the dependence on sensors for emulating tangible encounters in digital environments. The ability to position the user in physical space is a crucial requirement for AR/VR applications. In order to present appropriate digital overlays, AR applications must possess the ability to comprehend the user's spatial orientation with respect to geographical locations and physical objects. This entails the placement of instructions on a machine or the display of a virtual sign in front of a building. In the context of AR, it is imperative for devices and applications to obtain data pertaining to the user's spatial orientation and environmental factors in order to ensure their physical well-being. For the purpose of notifying users when they are in proximity to an object or when they cross predetermined boundaries, applications depend on the persistent awareness of a VR device regarding the user's location and the presence of any potentially dangerous objects or physical obstructions. In order to attain spatial awareness, AR/VR devices gather a diverse array of observed data pertaining to the location of the user. The data collected from various sources such as GPS, IMU, gyroscope or accelerometer, mobile devices camera,

[234] Cyber Civil Rights Initiative, '46 States + DC + One Territory Now Have Revenge Porn Laws' <https://wwwcybercivilrights.org/revenge-porn-laws> accessed 2 June 2023.
[235] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* 27 October 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 2 June 2023.

or external-facing cameras on a HMD, lidar, and other spatial sensors provide information about the user's physical position and their surroundings.

AR/VR devices not only gather data on a user's physical location, but also monitor specific movements and record biometric data to simulate the user's actions within a virtual environment. The type of empirical data holds significant value in the realm of VR, as the user is completely engrossed within a simulated environment. Fully virtual spaces are required to reconstruct physical experiences since their users do not possess any tangible landmarks to orient themselves, unlike physical space. The conversion of commonplace human experiences such as standing on stable ground, tactile interaction with objects, and the ability to move in various directions, among others, into a digitally rendered environment is a necessary process. This involves the translation of sensory inputs, head and eye movements, and other factors into a virtual space. The level of immersion experienced by users is directly proportional to the accuracy of the reconstruction. The attainment of immersive simulation by devices and applications is facilitated through the real-time collection of observed data pertaining to a user.

Further, HMDs and controllers can monitor the movements of the user's head and arms, and subsequently reproducing them within the virtual environment. Headsets with rudimentary capabilities are capable of monitoring motion through 3DoF, which correspond to three distinct types of head rotation (namely, horizontal, vertical, and lateral movements). Systems capable of replicating motion in 6DoF, encompassing the three rotational axes for head movement and full-body motions such as standing up, sitting down, shifting laterally, and moving to and fro, provide a more authentic representation of the movements of the user's in 3D space.[236] Certain immersive technologies also employ external sensors or cameras to perceive and monitor hand and finger motions in order to enable individuals to engage within the virtual interface and virtual objects of their immersive technology devices sans the utilization of controllers.[237]

Eye-tracking technologies, which utilize internal cameras to gather observed data pertaining to the user's gaze direction, alterations in their pupil dilation, and the state of their eyes being open or closed, have the potential to enhance the level of realism in immersive experiences.[238]

---

[236] Kei Studios, 'A Quick Guide to Degrees of Freedom in Virtual Reality' <https://kei-studioscom/quick-guide-degrees-of-freedom-virtual-reality-vr> accessed 3 June 2023.

[237] Meta Quest Blog, 'Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR," (*Meta,* 25 September 2019) <https://www.meta.com/blog/quest/introducing-hand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed 3 June 2023.

[238] HTC, 'HTC's VIVE Eye Tracking data collection: HTC Terms: Learn More' https://wwwhtc.com/us/terms/learn-more accessed 20 June 2023.

This data enables software applications to present avatars that are more authentic, accurately reflecting the user's eye movements and facial expressions. The utilization of gaze-tracking capabilities in VR displays enables the implementation of foveated rendering, a technique that emulates the human field of vision by reducing the resolution of displays that would be visible in a user's peripheral vision in the real world.[239] In addition to enhancing the realism of the experience and mitigating ocular fatigue, this approach can facilitate the production of superior quality visuals at the point of focus and diminish latency, a significant factor in the onset of motion sickness during immersive encounters.[240] BCI technologies are considered to be more sophisticated than eye tracking. The term refers to the utilization of sensors that gauge brain activity to promptly respond and adjust to the neural signals of a user. These encompasses extrinsic sensors, such as EEG sensors that are mounted on the head, in addition to prospective neural implants. Regarding AR and VR, the envisioned consumer brain-computer interface technologies are commonly comprised of sensors that are integrated into a wearable device, such as a headset. Although BCI technologies have not yet been integrated into commonly used consumer AR/VR devices, they present intriguing prospects for the field of AR/VR. These signals could be utilized by an immersive service or game to dynamically tailor experiences to better align with the individual requirements of a user in real-time.[241] A wearable AR device, equipped with a BCI, has the potential to be operated discreetly by the user through subtle gestures. To achieve this objective, AR/VR devices must gather raw data from neural activity sensors, which can be integrated into HMDs or obtained from other wearable sensors.

AR/VR technologies and applications enhance the user experience by incorporating additional information to complement sensor-based data. The provision of biographical information by users, including age, gender, affiliations, and interests, enables those services which provide customized experiences that cater to the specific needs of individual users. Additionally, the use of identifying information such as names or linked social media profiles serves to authenticate unique users and further integrates their virtual environments with the physical world, facilitating the development and expansion of social networks. Apart from the

[239] VIVE Enterprise, 'VIVE Pro Eye Office' https://enterprisevive.com/us/product/vive-pro-eye-office accessed 4 June 2023.
[240] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 4 June 2023.
[241] Scott Hayden, 'Valve Psychologist: Brain-Computer Interfaces Are Coming & Could Be Built into VR Headsets' (*Road to VR,* 23 March 2019) <https://wwwroadtovr.com/valve-brain-computer-interfaces-vr-ar-gdc-2019> accessed 4 June 2023.

information provided by the user, numerous AR/VR devices and applications are designed to gather observed data pertaining to in-world or in-app behavior and activities. The utilization patterns, duration of engagement, and preferences for specific AR/VR devices or applications can potentially disclose sensitive personal information about the user. An individual may participate in a support group within a social AR/VR application or attend an event tailored towards individuals with particular interests, affiliations and preferences.

Observed data refers to any documented evidence of an individual's involvement in a particular activity. These functionalities not only facilitate and enrich immersive experiences, but also broaden the scope of their applicability. Empirical research has demonstrated that the utilization of eye tracking technology can facilitate the diagnostic process of specific neurological conditions by mental health professionals. The integration of this technology in AR and VR devices presents novel prospects for their application in the healthcare industry.[242] Sensor-enabled VR can be utilized by market researchers to collect data analytics pertaining to consumer attention and product interaction.[243] In the interim, data obtained through device observation has the potential to enhance the safety and security of AR and VR devices and encounters. The utilization of biometric data, such as iris signatures, can prove to be a highly efficacious method for user authentication. Additionally, biographical, or behavioural data can serve to enhance in-app or in-world safety measures, for instance, by restricting access to age-appropriate content.[244] As the utilization scenarios and user demographics expand and become more varied, the potential applications of this observed data will also increase.

Like the case with observable data, one of the main issues regarding privacy that arises from observed data pertains to the preservation of individuals' anonymity and autonomy. The information contained in this data has the potential to unveil a considerable number of details pertaining to the lives of users, which may vary in terms of their degree of sensitivity. The data that users provide, ranging from biographical or health information to web-browsing or shopping history, has the potential to reveal or infer private details such as demographic information, residential location, and leisure activities. Similarly, to observable data, the

[242] Tia Ghose, 'Eye Tracking Could Diagnose Brain Disorders' (*Live Science*, 18 September 2012) <https://wwwlivescience.com/23274-eye-tracking-gaze-brain-disorders.html> accessed 4 June 2023.
[243] Albert Liu, 'Why VR Analytics is Critical to Prove ROI' (*cognitive3D blog*, 3 December 2019) <https://contentcognitive3d.com/vr-merchandising-case-study> accessed 4 June 2023.
[244] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail' (*VICE*, 28 May 2019) <https://wwwvice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 4 June 2023; The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.*, September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 4 June 2023.

discernibility of perceived information is subject to variation among users. Sharing geolocation data with friends and family may be perceived as advantageous and low-risk by certain users, but it may pose a threat to highly susceptible populations, such as children or individuals who have experienced abuse.[245] Likewise, certain individuals may opt to disclose personal identifying details, whereas others may choose to maintain anonymity. Revealing such information may potentially result in detrimental discrimination for certain users. The aforementioned scenario gives rise to a significant apprehension regarding privacy for those individuals who are susceptible to discriminatory acts, particularly in relation to employment opportunities or the ability to avail essential services, owing to their inherent characteristics such as gender, age, race, disability, sexual orientation, and other similar factors.[246] In the absence of protective measures to mitigate such discriminatory practices, the disclosure of such discernible data can result in substantial detrimental consequences. The employment of AR/VR devices and applications results in similar hazards emanating from the collected observed data. The sensitivity and potential of the information to cause harm vary significantly due to the vast amount of data collected. The potential hazards that individuals may encounter in relation to AR/VR technologies are contingent upon the specific manner, location, and objective for which they utilize said technologies. The sensitivity of biographical and health data of a patient observed through AR/VR therapies is expected to be higher compared to the same information disclosed by a user on a VR gaming or fitness platform. Additionally, the sensitivity of observed information about a user's location or surroundings would vary depending on the context, with information gathered in a private setting such as a living room being more sensitive than that collected in a public park or a shopping mall.

Due to the extensive scope of the gathered observed data, there is no universal strategy for addressing the privacy issues associated with this category of data. Moreover, this data confers substantial worth to numerous digital commodities, and in numerous instances, it is indispensable for their fundamental operations. The act of concealing, anonymizing, or limiting the collection of user data would significantly diminish the caliber of these services. In fact, it may render them ineffectual and impede the progress of any technology that relies on user-

[245] Daniel Christensen and Diana Jimenez, 'Data Protection Should Extend to Virtual Places and Data Objects' (*IAPP Privacy Perspectives, 24 August 2016*) <https://iapporg/news/a/data-protection-should-extend-to-virtual-places-and-data-objects> accessed 4 June 2023.

[246] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* 27 October 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 4 June 2023.

provided information. Achieving a balance between privacy concerns and functionality is crucial when contemplating mitigation strategies for observed data. The implementation of transparency, disclosure, and user consent is crucial in reducing the likelihood of negative consequences arising from the use of observed data. Users can make informed decisions regarding the information they choose to share, either directly or through opt-out/opt-in options, when they comprehend the methods and rationales behind the collection and sharing of their data by different AR/VR services. Users can modify their personal privacy settings according to their own subjective preferences regarding which information they wish to keep confidential, in addition to the information that is publicly available.

Nevertheless, it is not feasible to constrain all the observed data without compromising or interrupting the provision of the service. AR/VR devices necessitate motion-tracking data to simulate physical movements in virtual space, whereas a search platform may employ geolocation information to furnish more pertinent outcomes. In such instances, imparting knowledge to users regarding the ways in which their data is utilized by devices and applications to offer diverse services can empower them with greater control over their personal risk. Establishing unambiguous protocols for the storage and manipulation of data by AR/VR applications, along with specifying the circumstances, timing, and authorized personnel who may access it, can effectively reduce the potential privacy hazards associated with the collection of such data. In numerous cases, particularly those involving highly sensitive data such as biometric identifiers or sensitive health information, it is possible for the AR/VR application to process the data solely on the local device without transferring any data to a third party. Alternatively, data may be stored in the cloud only when the user has complete control over the encryption keys, thereby minimizing the risk of misuse. In some cases, data may be externally shared or stored without human observation.

The collection of data by products and services can facilitate the establishment of access and storage thresholds, which may be incorporated into transparency and disclosure protocols. Ultimately, the implementation of laws and regulations can serve as a safeguard for users in mitigating potential risks stemming from the inappropriate utilization of collected data. Various legal provisions exist to prevent discrimination against specific protected groups, irrespective of the means by which the discriminating party obtained information about an individual. In the states like the United States of America, there exist several laws that safeguard individuals

from being discriminated against in their employment based on characteristics such as race, gender, age, disability, and other similar attributes.[247]

Additional regulations exist that forbid discriminatory practices in relation to health insurance eligibility, housing, and various other services.[248] Regulations are implemented to regulate the confidentiality of users from government monitoring for the purpose of law enforcement. The Fourth Amendment of the US constitution safeguards individuals against unreasonable searches and seizures, and judicial precedents have broadened its scope to encompass observed data, such as location information.[249] The regulations aim to mitigate potential hazards associated with the divulgence of specific identifiable data during the utilization of online platforms.

3.3.2.3. COMPUTED DATA

In contrast to data that is observable or observed, computed data is not inherently furnished by users. Instead, it is the outcome of manipulating the information that users generate and observe, with the aim of deriving novel insights.[250] Computed data is utilized to analyze information from various sources in order to make predictions or inferences about users. Consequently, it has the potential to offer a comprehensive depiction that can be utilized to customize products and experiences for individual users. It is possible that it may be incorrect. The data that is generated through computation may encompass biometric identification, advertising profiles that are constructed based on a range of individual activities, or any other information that is deduced or construed rather than being explicitly furnished. The computational processes are essential for AR/VR devices to extract and utilize the copious amounts of raw data collected through their diverse sensors and user inputs.

AR and VR technologies gather a substantial quantity of both observable and observed data, which can subsequently be analyzed to offer more sophisticated functionalities and customized

[247] US Equal Employment Opportunity Commission, 'Laws Enforced by EEOC' (*eeoc.gov,* 10 February 2021) <https://wwweeoc.gov/statutes/laws-enforced-eeoc> accessed 4 June 2023.
[248] US Department of Justice Civil Rights Division, 'The Fair Housing Act' (*justice.gov,* 10 February 2021) <https://wwwjustice.gov/crt/fair-housing-act-1> accessed 4 June 2023; US. Department of Labor Employee Benefits Security Administration, 'FAQs on HIPAA Portability and Non-discrimination Requirements for Employers and Advisers' (*U.S. Department of Labor*) <https://wwwdol.gov/sites/dolgov/files/ebsa/about-ebsa/our-activities/resource-center/faqs/hipaa-compliance.pdf> accessed 4 June 2023.
[249] Louise Matsakis, 'The Supreme Court Just Greatly Strengthened Digital Privacy' (*Wired,* 22 June 2018) <https://wwwwired.com/story/carpenter-v-united-states-supreme-court-digital-privacy> accessed 4 June 2023.
[250] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* 27 October 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 4 June 2023.

user experiences. The amalgamation and analysis of descriptive data pertaining to users, including demographic details, geographical location, and in-app/in-world conduct or pursuits, can be utilized to customize advertisements, suggestions, and content to suit the preferences of individual users. As an illustration, an application could deduce, with varying degrees of accuracy, that individuals who engage in virtual dog play within a game possess a proclivity towards pets, and subsequently aim advertisements for pet-sitting services towards this cohort. Likewise, this data can be utilized to produce analytics that are presented to the user, such as approximating the number of calories expended during a workout by utilizing demographic data provided by the user and observed data on physical activities. AR/VR devices have the capability to produce computed data through the utilization of multiple sensors integrated within them. Hand-tracking technologies employ machine learning algorithms to estimate crucial information such as the size, shape, and positioning of a user's hands and fingers based on observed images of the hand.[251] Computed biometric identification methods, such as iris scanning or facial recognition, can be utilized by users to enhance the security of their applications and devices. In forthcoming devices enabled with BCI, the processing of neural signals into actionable commands will lead to the computation of data.[252]

The data that is computed differs from the information that is observed and observable in that it is primarily intended for the parties responsible for its production. As a result, it is not available to or able to be duplicated by external parties. Therefore, the privacy implications arising from computed data are less straightforward, yet more intricate. Users' comfort levels with the compilation and processing of their information may vary, but the potential for harm is contingent upon the manner in which the information is utilized, rather than solely on the individuals who are able to view or obtain it. The deductions or anticipations that constitute computed data possess the potential to unveil more delicate or possibly harmful details regarding a user than the distinct observed and observable information employed to produce them. The act of observing biometrics has the potential to yield supplementary information pertaining to a user's physical characteristics or medical status.[253] The security of computed

[251] Shangchen Han et al, 'Using Deep Neural Networks for Accurate Hand-Tracking on Oculus Quest' (*Facebook AI*, 25 September 2019) <https://aifacebook.com/blog/hand-tracking-deep-neural-networks> accessed 4 June 2023.
[252] Scott Stein, 'Mind Control Comes to VR, Letting Me Explode Alien Heads with a Thought' (*cnet*, January 30, 2021) <https://wwwcnet.com/news/controlling-vr-with-my-mind-nextminds-dev-kit-shows-me-a-strange-new-world> accessed 5 June 2023.
[253] Jacob Leon Kroger et al, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' (2020) IFIP Advances in Information and Communication Technology 576 <https://doiorg/10.1007/978-3-030-42504-3_15> accessed 5 June 2023.

data and the potential for unauthorized access by third parties are significant privacy concerns due to the sensitive nature of biometrically derived information. Unauthorized revelation of such data without the explicit permission or awareness of the user can result in considerable damage to one's reputation or cause embarrassment, particularly when the nature of the deduced information is of a sensitive or personal nature. Moreover, there exists the possibility of direct harm resulting from the utilization of computed data to unjustly deprive an individual of specific services or opportunities. These encompasses instances of prejudice in various domains, including but not limited to housing, employment, insurance, benefits, and other services, which stem from the accurate inference of personal information pertaining to an individual, such as their age, gender, sexual orientation, or health status. The detriments may ensue in cases where imprecise computed data, such as an erroneous credit rating, precludes an individual from availing themselves of services for which they meet the eligibility criteria. The privacy risks associated with computed data are especially pronounced in the realm of AR and VR. These technologies have the capability to collect a diverse array of observable and recorded data, which may encompass confidential biometric data. However, if this information is utilized without limitations, it has the potential to unveil substantial and extremely sensitive supplementary details about an individual. This encompasses deduced information regarding inclinations from involuntary or subconscious gestures or responses, along with the recognition of personal, demographic, and health-related data.[254] The unregulated collection and analysis of this data may lead to the identification of exceedingly precise details pertaining to individuals. The vast potential AR and VR technologies in generating computed data is advantageous for their utilization and technological progression. However, in the absence of appropriate protective measures, these technologies can pose a threat to users' safety.

The potential negative consequences of privacy breaches resulting from computed data primarily stem from inadvertent utilization, unapproved entry, or malevolent exploitation. The objective of mitigation strategies is to safeguard deduced data that has not been explicitly furnished or produced by the user, and provide redress for any resulting damages. Like other forms of data, the fundamental basis for any strategy aimed at mitigating computed data involves the disclosure and consent of users. It is imperative that users possess a comprehension of the inferences that can be drawn from the data they furnish, as well as the way said data is utilized. User privacy preferences can enable individuals to opt out of certain data aggregation and computing for inferred data that is not integral to the fundamental operations of a device

[254] Ibid.

or application. In cases where inferred information is integral to the functionality or quality of services, it is imperative to maintain transparency and disclosure regarding the utilization of such information. This approach can facilitate users' comprehension of the data practices that are being employed. In addition, like the handling of observed data, well-defined protocols specifying the storage of data and the conditions under which it can be accessed, as well as the authorized personnel who can access it, serve to safeguard users against potential personal or reputational risks that may arise from unauthorized access. In addition to the practices, alternative mitigation strategies can be employed to tackle the tangible negative consequences that users may encounter as a result of computed data, including but not limited to discriminatory outcomes. The enactment of laws prohibiting discrimination based on computed data assumes significance owing to the possibility of such data revealing sensitive information that users may not be willing to divulge.

Notwithstanding the existence of nondiscrimination laws, the potential negative consequences arising from the erroneous deduction of information, such as the implementation of unfavorable measures predicated on an imprecise credit score, may not always be fully mitigated. Enabling users to rectify inaccurate or obsolete information can serve as an additional measure to mitigate such hazards. Given the increasing prevalence of AR/VR devices, it is imperative to contemplate strategies for mitigating computed data in contexts beyond individual or recreational use. Instances may arise where employers mandate their staff to undergo training that employs this technology, or academic institutions may furnish their students with headsets for the purpose of educational enhancement. These activities have the potential to produce substantial computational data regarding employees or students during their implementation. When usage is obligatory, individuals are unable to provide significant consent for the gathering of data. It may be imperative to establish restrictions on the modalities and temporalities in which third-party entities, such as service providers, employers, or instructors, are authorized to obtain or employ the data.

3.3.2.4. ASSOCIATED DATA

The last classification of user data that has the potential to pose privacy threats is associated data. In contrast to other forms of user data, associated data does not furnish descriptive information. Stated differently, the presence of associated data alone does not provide any

precise information pertaining to an individual user.[255] The data encompasses details such as identification, registration, and account numbers, device, and login particulars, and addresses or other forms of contact information. The utilization and generation of data by AR/VR devices may pose privacy risks when combined with other information or exploited for nefarious purposes.

Whilst AR/VR technologies may present innovative applications and immersive encounters, they are essentially a type of interconnected device, comparable to laptops and IoT devices. AR/VR technologies can gather and produce user-related data as they function as interconnected devices, such as wearable headsets or AR-enabled mobile devices. The associated data provided by users encompasses various particulars, including login credentials (e.g., usernames and passwords) for applications and services, user contact details such as email, phone number, and residential address, and user payment particulars such as bank account numbers and credit card information. Data that is associated with users can also be produced as a result of their activities within the application or virtual environment. The associated data, such as lists of "friends" or other connections, on social or multiuser AR/VR platforms can disclose information regarding a user's social connections and activities.

Likewise, digital media and virtual assets that do not disclose personal identity are also considered as correlated data. These encompasses visual captures and audiovisual documentation of virtual environments, either in their entirety or in part, produced by the users themselves. These materials may be disseminated publicly or withheld for personal use. An individual can take a photograph of a digital object within their residence by utilizing a smartphone or a heads-up AR device. Apart from AR and VR renditions of digital media, entirely virtual entities can also serve as related data. This encompasses virtual spaces that are either partially or fully created by users, virtual objects or overlays that are shared through augmented reality, and objects that users can engage with through immersive experiences. The provision of such information is imperative for the purpose of linking users with their distinct accounts, user preferences, and digital possessions. In order to furnish user-specific information, such as recently accessed applications and social interactions, a device necessitates a mechanism for user recognition and authentication, which is commonly achieved by a username or email address and password. The inclusion of payment information is

[255] Daniel Castro and Alan McQuinn, 'ITIF Filing to FTC on Informational Injury Workshop' (*Information Technology and Innovation Foundation,* 27 October 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 5 June 2023.

imperative for any device or application that facilitates user transactions, particularly those involving the acquisition of paid content. AR and VR devices are typically accompanied by associated data, including registration numbers and IP addresses. Like the way a username and password authenticate an individual's identity, this data serves to identify a device and facilitate its ability to perform tasks that necessitate an online connection. The device information is linked to the user; however, it does not provide direct identification or description of the user on its own.

When utilized exclusively by authorized parties, associated data poses minimal privacy risks to individuals. Nonetheless, within the broader framework of user data, correlated information has the potential to result in negative consequences. The aggregation of descriptive data collected by a specific device or service can potentially unveil supplementary information that a user may prefer to keep private. The combination of a screen name or user ID with identifying information has the potential to establish a connection between an individual and specific actions, such as their browsing history. In certain cases, the IP address of a device can disclose the user's identity and associate them with specific Internet-enabled actions.[256] The disclosure of linked information may result in reputational damage or personal autonomy infringement, depending on its nature and sensitivity. The misuse of associated information by malicious actors can result in negative consequences. Although a username and password may not contain substantial personal information, they can serve as a gateway to confidential accounts ranging from social media to financial services. Fraudulent activities can result in both financial and non-financial damages, thereby causing negative impacts on the economic and reputational aspects. Insufficient measures to protect associated information can result in substantial negative consequences that are frequently challenging to rectify. Numerous hazards are also prevalent in the realm of AR and VR, and in certain instances, they may be intensified by the magnitude of data that can be amalgamated with related information. An instance of ill-intentioned behavior could involve the utilization of linked authentication information to not solely gain entry to a user's account, but also to assume their identity in the digital realm.

Efficient strategies for mitigating the risks of harm associated with this data primarily involve measures that guarantee authorized access to and usage of the information, while also restricting its integration with other descriptive or identifying data. In certain cases, amalgamating identifying information with correlated data can safeguard users against risks by

[256] Nefi Acosta, 'Are IP Addresses 'Personal Information' Under CCPA?' (*IAPP Privacy Advisor*, 28 April 2020) <https://iapporg/news/a/are-ip-addresses-personal-information-under-ccpa> accessed 5 June 2023.

means of enhanced user authentication. In instances where a biometric identifier, such as a fingerprint, is linked to a username and password, the potential for malicious actors to exploit the associated information for fraudulent purposes is reduced. Legal frameworks and regulatory measures pertaining to information security can serve as a safeguard against malevolent exploitation of users' data, or alleviate the negative consequences in the event of unauthorized access by malicious entities. The encompasses regulations pertaining to both the safeguarding of information and the protection of data, as well as the obligation to notify users in the event of a data breach that may have compromised associated sensitive data. The implementation of standards for disclosure, transparency, and consent can effectively reduce potential risks of harm by providing users with notification when a product or service amalgamates their associated data with other information, including identifiable data.

3.3.3. PRIVACY CONSIDERATIONS SPECIFIC TO USERS IN THE CONTEXT OF AR/VR

3.3.3.1. INTRODUCTION

The extant frameworks and mitigation approaches pertaining to privacy concerns provide a significant basis for tackling user privacy in the context of AR and VR. Nevertheless, these aforementioned factors are inadequate in comprehensively tackling the unprecedented hazards that are associated with immersive technologies. The collection and processing of user data in immersive, multimodal AR/VR devices and applications is distinct from other forms of digital media due to its heightened scale and sensitivity. Both AR/VR platforms and other digital media can share and record videos that are observable in real time. However, immersive recording provides more advanced capabilities that necessitate extensive data collection, such as gaze and motion tracking, and the integration of associated information through virtual assets.[257]

Collaborative AR and VR applications, including multiplayer games, social experiences, training simulations, virtual classrooms, and remote office solutions, will necessitate the establishment of novel standards and anticipations concerning privacy and conduct. These standards and expectations are not currently present in other platforms, such as social media and videoconferencing, or in face-to-face interactions involving one-on-one or small groups.

[257] XR Safety Initiative, '341.1: FERPA: Protection of Education Record Considerations' (*The XRSI Privacy Framework Version 1.0.*, September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf > accessed 5 June 2023.

The utilization of AR/VR platforms will result in the production of substantial quantities of observed and observable data, encompassing various aspects such as conversational intricacies, individual locomotion, and even physical reactions within the virtual realm.[258] According to a study, the level of immersion in a platform is directly proportional to the likelihood of individuals perceiving a false sense of privacy. This may lead them to overlook the possibility of their actions being exposed to a larger audience than anticipated.[259]

The acquisition and utilization of data in AR/VR technology raises unique issues that span the four data categories, necessitating meticulous examination. The vast assortment of biometric data and its capacity to unveil personal information beyond mere user identification pose privacy obstacles that are unique to other biometric information technologies. Furthermore, the comprehensive scope of this data gathering and the opportunities it provides render numerous current mitigation strategies inadequate or unfeasible for implementation within this framework. The collection of sensitive data and the immersive qualities of AR/VR experiences have the potential to amplify pre-existing risks for vulnerable users, resulting in acute harms.

3.3.3.2. DISCUSSION ABOUT THE RELATIONSHIP BETWEEN BIOMETRIC DATA AND THE PERSONAL AUTONOMY OF USERS OF IMMERSIVE TECHNOLOGY

The emergence of AR/VR technology presents novel challenges to the preservation of user agency and privacy. In contrast to other digital media formats, immersive technologies necessitate the complete or partial translation of various facets of identity of a user and actions from the physical realm to the virtual domain. This encompasses not only facets of an individual's identity, such as biographical data or interests and associations, but also particulars regarding their whereabouts, mobility, physical attributes, physiological reactions, and other data. The integration of “real” identity information which is provided by users of such tech along with subtle features that is observed through their in-app activity can effectively reveal undisclosed information about their activities, interests, and preferences.[260]

In the context of AR/VR usage, individuals who engage in fully immersive experiences tend to view their virtual representations as an integral aspect of their personal identity, rather than

[258] Fiachra O’Brolchain et al, ‘The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy’ (2015) Springer Link <https://link.springer.com/article/10.1007/s11948-014-9621-1> accessed 5 June 2023.
[259] Ibid.
[260] Brittan Heller, ‘Reimagining Reality: Human Rights and Immersive Technology’ (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 5 June 2023.

as a distinct or supplementary entity. The increasing prevalence of photorealistic avatars, especially in non-entertainment contexts, may lead to virtual identities that closely resemble their real-life counterparts.[261] The precision of this depiction is further enhanced by incorporating motion, gesture, and gaze-tracking technologies that simulate a user's bodily reactions in their digital surroundings. The capacity to replicate an individual's facial expressions and responses in virtual environments amplifies the quality of interactions, but necessitates users to disclose and authorize devices to collect, monitor, and analyze a significantly greater amount of data than other digital media platforms that solely transmit audiovisual content. The collection of "nonverbal data" through tracking subtle and subconscious movements that can be detected by sensors is highly resistant to conscious control by users.[262]

The adoption of immersive identities in virtual environments precludes users from achieving complete anonymity while navigating such spaces. Upon the integration of identifying information, such as a complete name, with biometric identification data derived from eye-tracking cameras, the process of completely anonymizing a user becomes exceedingly challenging, even in the absence of the identifying information.[263] The conflation of observable, observed, computed, and associated data exacerbates the potential for harm by rendering them indistinguishable.

One of the most notable differences between immersive technologies and other forms of digital media is the former's utilization of biometric data to simulate physical experiences within a virtual environment. When considered in isolation and devoid of contextual information, the data elicits minimal apprehension among policymakers and privacy experts, who have previously voiced similar concerns regarding other technologies, such as mobile phones and IoT devices. The capacity of AR/VR devices to collect and analyze vast amounts of biometric data gives rise to novel hazards. According to estimations made by the Stanford Virtual Human

[261] Ibid.
[262] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics,* August 6 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 11 June 2023.
[263] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail' (*VICE*, 28 May 2019) <https://wwwvice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 11 June 2023; The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.*, September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 11 June 2023.

Interaction Lab, users can produce nearly 2 million distinct recordings of bodily expressions during a single 20-minute VR session.[264]

In the event of authorization, AR/VR technologies and software have the potential to deduce substantial supplementary data that discloses identifiable biographical and demographic particulars, irrespective of a user's decision to furnish such information. The utilization of eye-tracking technologies enables the collection of observed data that not only discloses an individual's visual focus and gaze, but also provides insight into personal characteristics such as age, gender, and race.[265] Additional data, such as motion or hand tracking data, possesses the capability to distinguish individuals with a high degree of accuracy. According to a study, a mere five-minute collection of 6DoF tracking data in a standing position was adequate to accurately re-identify individuals with up to 95% precision, even when conducted across multiple sessions.[266] Applications have the capability to utilize biometric data to deduce information regarding a user's physical and emotional reactions to stimuli, in addition to confidential health-related data. The utilization of motion and eye tracking technology has the capability to capture a user's subconscious reactions, including pupil dilation. This information can subsequently provide insight into inferred details regarding their interests and preferences, ranging from preferred cuisine to sexual orientation.[267]

While the collection of biometric data is not exclusive to AR/VR technology, the extent of data gathered and the possibility of deducing supplementary information is unparalleled in other consumer devices designed for utilization beyond regulated environments. In the absence of adequate protective measures, the psychographic profiles derived from this data have the potential to result in negative consequences, such as instances of prejudice and encroachments upon individual autonomy.[268] The disclosure of sensitive information and private details that an individual did not intend to reveal can occur through their inadvertent disclosure. Moreover, there may be supplementary negative consequences that can emerge as a result of unapproved

[264] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics,* August 6 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 11 June 2023.
[265] Joseph Jerome, 'Establishing Privacy Controls for Virtual Reality and Immersive Technology,' (IAPP Privacy Perspectives, *September 9, 2020*) <https://iapporg/news/a/establishing-privacy-controls-for-virtual-reality-and-immersive-technology> accessed 11 June 2023.
[266] Mark Roman Miller et al, 'Personal Identifiability of User Data During Observation of 360-Degree VR Video' (2020) 10 Scientific Reports <https://doiorg/10.1038/s41598-020-74486-y> accessed 12 June 2023.
[267] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail' (*VICE*, 28 May 2019) <https://wwwvice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 12 June 2023; The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.,* September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 12 June 2023.
[268] Ibid.

retrieval of an individual's biometric identification data. While biometric data, such as fingerprints, may not inherently disclose personal or identifying details, it can be linked to a specific user for purposes of authentication or identification. The involvement of a significant amount of biometric data in AR/VR raises a noteworthy privacy concern with regards to information security.

3.3.3.3. CONSTRAINTS ON EXISTING MITIGATION PRACTICES & APPROACHES

The immersive characteristic of such technologies poses a challenge for standard mitigation approaches aimed at limiting potential harms associated with various types of data. The assessment of consent, transparency, and disclosure measures that prioritize the user are more intricate in the context of AR and VR technologies compared to other digital and interconnected technologies. The interaction of users with fully or partially virtual spaces differs from that on 2D platforms, which implies that conventional consent practices may require a rethinking for immersive experiences.[269] In immersive experiences, users may encounter difficulties in accessing hyperlinks or providing explicit consent due to the nature of the environment.[270] Furthermore, although privacy preferences afford users the option to abstain from sharing or withhold certain information, there exist notable constraints to this strategy given that sensitive or potentially identifiable data is indispensable to the fundamental operations of immersive technologies.

Secondly, the process of anonymizing data poses a significant challenge due to the abundance of identifying information that is both provided and generated by users. Despite the de-identification of tracking data by means of name removal, the raw biometric data remains susceptible to re-identification of users through their distinctive movements.[271] In order to achieve genuine de-identification of sensitive biometric and biometrically derived data, it is imperative to implement supplementary measures beyond mere name removal.[272] The

[269] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics*, August 6 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 12 June 2023.
[270] Erin Egan, 'IIC: New Technologies and Interfaces in Communicating About Privacy: Towards People-Centered and Accountable Design' (*Facebook*, July 2020) <https://aboutfb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf> accessed 12 June 2023.
[271] Jessica Outlaw and Susan Persky, 'Industry Review Boards are Needed to Protect VR User Privacy' (*World Economic Forum*, August 29, 2019) <https://wwwweforum.org/agenda/2019/08/the-hidden-risk-of-virtual-reality-and-what-to-do-about-it> accessed 12 June 2023.
[272] Ann Cavoukian and Daniel Castro, 'Big Data and Innovation, Setting the Record Straight: De-Identification Does Work' (*Information Technology and Innovation Foundation*, 16 June 2014) <https://www2.itif.org/2014-big-data-deidentification.pdf> accessed 12 June 2023.

significance of secure storage and well-defined access boundaries is heightened, thereby prompting inquiries regarding the advantages and drawbacks of diverse data management methodologies. The paramount inquiries pertain to the accessibility of the user's data by either the user or a third-party and to investigate the adequacy of the measures which were implemented to ensure the security of the data.[273]

The adequacy of extant legal protections to mitigate the potential hazards arising from the collection of diverse data in AR/VR remains uncertain. Although legal measures exist to deter the dissemination of nonconsensual pornography, they typically do not safeguard individuals from the negative consequences of virtual reproductions of themselves or their virtual assets, such as anonymity and autonomy harms. The existence of a policy gap is discernible in the widespread prevalence of "deepfakes," which are artificially generated media that imitates the appearance of a person. This has resulted in apprehensions regarding the protection of personal autonomy and the entitlement to publicity from digital replicas. An instance of this can be observed in the proposition of a bill by the New York State legislature, which aims to broaden the scope of rights to publicity by encompassing digital replicas. This proposed legislation seeks to impose limitations on the utilization of said replicas for trade or commercial purposes.[274] Nonetheless, this peril is particularly accentuated in immersive encounters, where the technological complexity of artificial media may not be a prerequisite. If an individual gains unauthorized control over another individual account, they can create an illusion of non-consensual action on behalf of the victim. In addition to unauthorized access, it is possible for malicious actors to fabricate a virtual presence by generating replica avatars and other virtual assets, given an adequate amount of observable information. The potential misuse of such a replica for fraudulent purposes and the consequent infliction of emotional, reputational, and economic damages are easily conceivable. Moreover, it is noteworthy that the legal safeguards such as rights of search and seizure in the United States have not been extended to virtual and augmented technologies if the State requests.[275]

---

[273] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology is Advertising's Holy Grail' (*VICE*, 28 May 2019) <https://wwwvice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 14 June 2023; The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.,* September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 14 June 2023.

[274] New York State Senate, 2017-2018 legislative session, A8155B <https://wwwnysenate.gov/legislation/bills/2017/a8155> accessed 15 June 2023.

[275] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (J*AMA Paediatrics,* August 6 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 15 June 2023.

3.3.3.4. AGGRAVATED SUSCEPTIBILITY OF VULNERABLE USERS TO POTENTIAL HARM

The collection of data cause disproportionate adverse impacts on certain vulnerable groups, such as the aged, children and marginalized sections of the society. Individuals belonging to certain groups face an increased likelihood of experiencing harm resulting from the exposure of their personal information, including but not limited to discrimination or violations of their autonomy. Simultaneously, these individuals may possess a comparatively lower level of proficiency in managing their personal privacy risks or providing fully informed consent for data collection. Considering the vast amount of data gathered in the realm of AR and VR, coupled with the possibility of its exploitation, it is pertinent to acknowledge the distinctive hazards posed to its most susceptible users. It is of utmost significance to consider the examination of potentially sensitive use cases, such as those in health care, child development, education, and certain workforce-training applications.

Individuals who are already vulnerable to negative consequences stemming from discrimination or compromised anonymity and autonomy are especially susceptible to such risks in the context of AR and VR. The utilization of AR/VR technology by individuals in health care research or mental illness therapy may produce both observed and computed data that possess the potential to result in discrimination in health care or employment if disclosed to service providers or employers. Elevated risks to the preservation of autonomy and anonymity are a significant area of apprehension. Inadequate protective measures may result in the generation of observed biometric data of individuals who are susceptible to discrimination or physical harm based on their age, sex, race, sexual orientation, or certain health conditions, thereby enabling the inference of such information without their explicit consent.

Secondly, it is imperative to contemplate the degree to which juvenile users possess the capability to grant complete consent to the gathering of data that occurs within immersive encounters. As previously mentioned, the task of converting conventional consent mechanisms into immersive, 3D systems is already a formidable undertaking. Similarly, conventional methods of ensuring age-appropriate content and safeguarding children's security on digital platforms, such as parental controls, age verification, and restrictions on personal data

gathering, hold true.[276] It is impractical to anticipate that children possess a comprehensive understanding of the scope and rationale behind the collection of personal data, which consequently impedes their ability to provide informed consent for its utilization. Moreover, children may lack the capacity to effectively distinguish between tangible and virtual components within immersive encounters, thereby increasing their vulnerability to potential harm resulting from the disclosure of personal information. Moreover, due to the fact that minors are unable to provide complete consent regarding the potential hazards associated with disclosing identifying or biometric data in the context of AR/VR, the absence of measures to address these risks during their formative years may result in prolonged negative consequences.[277] An instance of motion-tracking data obtained from a device utilized during an individual's childhood has the potential to be utilized in the future for the purpose of re-identifying said individual on a novel device or application.

3.3.4. THE REGULATORY FRAMEWORK GOVERNING USER PRIVACY IN THE CONTEXT OF AR/VR

3.3.4.1. INTRODUCTION

Despite the novelty of the technology, AR/VR devices and applications are currently subject to various legal and regulatory frameworks that address the protection of personal privacy and user data in countries such as the United States of America. In USA, the extant regulatory framework partially mitigates the hazards associated with AR/VR technology, while specific stipulations impede the acquisition of data essential for delivering immersive experiences that are both resilient and secure across various domains. Moreover, akin to the emergence of AR/VR, there are novel aspects to be considered in relation to safeguarding user privacy. Additionally, the implementation of policies to tackle these issues poses distinctive hurdles in the context of AR/VR technologies. The existing legal and regulatory frameworks pertaining to these technologies exhibit significant deficiencies in policy with respect to certain issues, while necessitating overly intricate solutions for others.

However, due to the presence of numerous numbers of legal regulations and provisions with respect to Privacy in realm of AR/VR in the USA. Let us take an example of such legal

[276] The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.,* September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 16 June 2023.
[277] Jessica Outlaw and Susan Persky, 'Industry Review Boards are Needed to Protect VR User Privacy' (*World Economic Forum,* 29 August 2019) <https://wwwweforum.org/agenda/2019/08/the-hidden-risk-of-virtual-reality-and-what-to-do-about-it> accessed 16 June 2023.

provisions and regulations of USA in order to understand the existing regulatory framework governing user privacy in AR/VR.

3.3.4.2. EXISTING LEGAL PROVISIONS & REGULATIONS ABOUT PRIVACY IN VIRTUAL SPACE

The existing regulatory framework governing user privacy in countries like United States which is a heterogeneous amalgamation of legislative measures at both federal and state levels seeks to address diverse issues. The National-level privacy regulations in the USA encompass provisions for safeguarding sensitive data and protecting vulnerable user groups, as well as stipulations for data collection and management by designated entities. The collection of data through immersive experiences is subject to regulation by COPPA, FERPA, and HIPAA. Notwithstanding, these regulations solely pertain to information objectives, as opposed to broader categories of information. COPPA imposes limitations on the gathering and retention of perceived and perceivable data, including personal details, recordings, and geospatial data, exclusively in commodities and amenities designed for minors.[278]

Regulations have been established to govern the utilization of digital data by the government of countries such as the USA, encompassing information collected through AR/VR technologies. The management of records pertaining to individuals by federal agencies, including data obtained through the use of AR/VR technologies, is subject to regulation under the Privacy Act of 1974.[279] Over the course of almost a hundred years, the legal system has established supplementary measures to ensure that law enforcement's utilization of personal and digital data, such as audiovisual recordings and specific types of metadata, is appropriately regulated.[280] To date, there exists a dearth of legal rulings that have specifically tackled the extent and magnitude of data that is collected and deduced from an AR/VR apparatus.

At the state level in the USA, several statutes exist pertaining to biometric privacy and the wider scope of data protection. The CCPA mandates compliance obligations for entities that engage in the collection, processing, and dissemination of personal information, encompassing biometric data, within the state of California. Although the CCPA does not explicitly mention

[278] US Federal Trade Commission, 'Complying with COPPA: Frequently Asked Questions' (*ftc.gov*, accessed 10 February 2021) <https://wwwftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 15 May 2023.
[279] US Department of Justice Office of Privacy and Civil Liberties, 'Overview of the Privacy Act of 1974 (2020 Edition)' (*justice.gov*, 10 February 2021) <https://wwwjustice.gov/opcl/overview-privacy-act-1974-2020-edition> accessed 16 May 2023.
[280] Louise Matsakis, 'The Supreme Court Just Greatly Strengthened Digital Privacy' (*WIRED*, 22 June 2018) <https://wwwwired.com/story/carpenter-v-united-states-supreme-court-digital-privacy> accessed 16 May 2023.

AR or VR, companies that offer these technologies have implemented a combination of measures that are tailored to meet regulatory requirements and more broadly applicable compliance standards.[281] The states of Illinois, Texas, and Washington have enacted legislation that specifically addresses the collection of biometric data and facial recognition technologies, mandating that notice and user consent be obtained prior to the gathering of such data.[282] The aforementioned circumstance presents an additional layer of complexity to the regulatory landscape and compliance obligations for AR/VR providers. Given the inherent characteristics of the technology, it is probable that these providers will be required to obtain certain types of biometric data from their users.

3.3.4.3. POLICY CHALLENGES THAT ARISE IN THE CONTEXT OF SAFEGUARDING USER PRIVACY IN THE REALM OF AR/VR

The utilization of AR/VR devices and applications necessitates a substantial amount of information, coupled with the delicate nature of said data. As a result, these technologies pose novel challenges to policy discussions concerning user privacy. The absence of a definitive standard for the quantity of data required to facilitate fundamental operations (as distinct from supplementary advantages that empower users to decide if they are ready to disclose personal information to access them) is apparent. The circumstance poses a challenge to the implementation of consent regulations that AR/VR providers may be subject to. The XR Safety Initiative, a collaborative effort involving multiple stakeholders, has raised concerns regarding the potential lack of agency for individuals to decline the processing of sensitive data, as well as the challenge of distinguishing between essential and non-essential data.[283] Moreover, due to its recent emergence, AR/VR technology is yet to garner significant consumer awareness regarding the rationale behind its extensive data collection. A forthcoming challenge involves distinguishing between adverse reactions, which can be mitigated through increased public awareness and comprehension, and the genuine possibility of harm arising from data collection. A significant proportion of individuals are amenable to relinquishing certain data in exchange for online services that are either free or available at a low cost.[284]

---

[281] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics*, 6 August 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 16 May 2023.

[282] Ross D Emmerman et al, 'New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies' (*Loeb & Loeb*, March 2018) <https://wwwloeb.com/en/insights/publications/2018/03/new-biometric-information-privacy-cases-reveal-b> accessed 16 May 2023.

[283] The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.*, September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 17 June 2023.

[284] Jeremy Bailenson, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics*, 6 August 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 18 June 2023.

An additional obstacle that policymakers encounter pertains to the delineation of the extent of personal information and confidential information. The present laws pertaining to the pertaining to the protection of personal, identifying, and biometric data are inadequate in addressing the comprehensive scope of sensitive information amassed in AR/VR, as well as its potential applications beyond user identification or authorization.[285] Moreover, the data protection regulations implemented in the United States and other countries aim to address the privacy concerns of individuals acting as data subjects. However, these regulations do not encompass the complete virtual spaces or assets within the definitions of "personal" or identifying information.[286] The application of established concepts of user privacy, which serve as the basis for privacy regulations and policies, presents a challenge in the realm of AR/VR. The broad objectives of privacy regulations can conceivably encompass AR/VR devices and applications. However, the strategies delineated in extant laws like the GDPR may not be directly transferable to, or indeed efficacious for, immersive experiences.

Ongoing framework for AR/VR technologies is characterized by a patchwork of standalone standards on specific technologies. Limitations on a particular category of data can have a significant impact on the overall functionality of the technology due to the extensive nature of data collection required. Several regulations are not applicable to immersive experiences and tend to limit certain uses while ignoring other potential hazards. The issue poses a significant policy dilemma, primarily in terms of elucidating the implementation of these regulations concerning AR/VR technologies. Additionally, it is imperative to synchronize these diverse regulations to prevent excessive constraints on the advancement and utilization of AR/VR devices and applications.

3.3.5. SUGGESTIONS AND ADVICE FOR PROTECTING PRIVACY UNDER IMMERSIVE TECHNOLOGY

The extent and magnitude of user data acquisition in the realm of AR/VR raise significant inquiries regarding safeguarding users against potential negative consequences, while simultaneously promoting the sustained advancement of this swiftly evolving technology. It is imperative for both policymakers and developers to strive for comprehensive measures that

[285] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 18 June 2023.

[286] Daniel Christensen and Diana Jimenez, 'Data Protection Should Extend to Virtual Places and Data Objects' (*IAPP Privacy Perspectives,* 24 August 2016) <https://iapporg/news/a/data-protection-should-extend-to-virtual-places-and-data-objects> accessed 18 June 2023.

incorporate essential protective measures and establish benchmarks for user confidentiality that can be implemented across current and forthcoming applications. The matter at hand necessitates meticulous examination of the constituent elements of AR/VR technologies, the categories of data they amass, and the plausible risks associated with such data. The current strategies implemented are expected to have a lasting influence on the development of AR/VR gadgets and software for various domains, including consumer, enterprise, and governmental sectors.

3.3.5.1. CREATION OF AN IMPARTIAL INNOVATIVE REGULATORY DIGITAL SPACE IN ORDER TO ADDRESS PRIVACY CONCERNS WITHIN THE DIGITAL DOMAIN

It is imperative for policymakers to establish a regulatory framework for AR/VR development that not only facilitates exploration of additional safeguards by developers but also ensures user privacy protections. As several conventional strategies for mitigating privacy issues arising from digital technologies and interconnected devices are not readily applicable to immersive experiences. It is recommended that policy measures refrain from impeding the capacity of AR/VR developers to devise inventive mechanisms aimed at alleviating privacy risks, such as those related to user consent, transparency, and choice.

3.3.5.2. ADVICE AND ELUCIDATION ON THE IMPLEMENTATION OF THE EXISTING PRIVACY LAWS IN THE VIRTUAL SPACE

As mentioned earlier, several regulations in the USA concerning data privacy are applicable to specific data in the context of AR/VR. Nevertheless, it is unclear to what degree the data collection practices of AR/VR conform to these regulations. The lack of clarity regarding the timeline and way AR/VR devices and applications ought to adhere to federal and state regulations has resulted in a state of regulatory ambiguity for companies involved in their development. Insufficiently defined directives may impede the progress of inventive ideas, especially in emerging domains that lack well-defined regulatory frameworks such as tracking and BCI technologies. Similarly, strictly regulated fields such as health data and products designed for children may not have direct applicability to AR and VR, thereby necessitating further interpretation. It is imperative that the pertinent federal agencies and regulatory bodies responsible for monitoring extant privacy regulations offer unambiguous directives regarding their implementation within immersive environments. It is recommended that the guidance should effectively amalgamate the current regulatory frameworks in a uniform manner at the

federal level, while also discouraging any additional fragmentation on a state-by-state basis. It is imperative for regulators to meticulously contemplate the data categories explicated in this report and their indispensability to pertinent AR/VR devices and applications. The Department of Health and Human Services in USA may also evaluate the categorization of "protected health information" under HIPAA for the data obtained through AR/VR technologies in healthcare, considering the observable, observed, and computed information. The FTC can provide further elucidation on the compliance of the COPPA with regards to the collection of data in the context of AR/VR. This includes determining the appropriateness of collecting audiovisual recording or geolocation data for the fundamental operations of AR/VR devices and applications, as the agency has previously done for voice recordings.[287]

3.3.5.3. RECOMMENDATION TO CONSIDER REFORMING PRIVACY LAWS WHICH IMPOSE UNNECESSARY LIMITATION ON THE USE OF AR/VR

Certain laws that were formulated with a particular technology or application in consideration may impose superfluous constraints on the progress of AR/VR innovation. The utilization of AR/VR devices and applications necessitates a substantial amount of information to execute rudimentary operations. Consequently, the regulatory measures designed for independent technologies may impose compliance criteria that are arduous or unfeasible for AR/VR providers to uphold. It is recommended that policymakers at the state level (in USA) undertake a review of data privacy laws that have been designed to cater to particular use cases or data collection practices. This review should aim to reassess any laws that may impose restrictive limitations on the utilization of AR/VR technologies. Of particular significance are the state statutes regulating biometric data, which are typically formulated to regulate biometric identification. However, these statutes may hinder the functionality of AR/VR systems that necessitate the use of observed biometric data, such as eye and motion tracking. It is recommended that Congress (in US) act at the federal level to mitigate the potential hazards of disparate state privacy regulations by implementing a cohesive national privacy framework that supersedes state laws.[288] Furthermore, it is imperative to give due regard to stringent data privacy regulations like COPPA. Restrictions on the collection of personal information, such

[287] US Federal Trade Commission, 'FTC Provides Additional Guidance on COPPA and Voice Recordings' (*ftc.gov*, 23 October 2017) <https://wwwftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings> accessed 18 June 2023.

[288] Alan McQuinn and Daniel Castro, 'A Grand Bargain on Data Privacy Legislation for America' (*Information Technology and Innovation Foundation*, 14 January 2019) <https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america/> accessed 18 June 2023.

as biographic information, voice recordings, and geolocation, may pose a significant challenge to the development of AR/VR devices and applications. This is since limiting the collection of certain types of data could potentially compromise the quality and functionality of the technology. Consequently, such restrictions could significantly curtail the potential of AR/VR technologies to be utilized in contexts that are focused on children. Simultaneously, implementing limitations may not inevitably safeguard minors from numerous possible detriments and confidentiality hazards that are distinct to or intensified by AR/VR technology. In multiplayer environments, children may encounter various risks such as harassment, exposure to inappropriate content, and divulging personal information to unknown individuals. Furthermore, it is recommended that the Federal Trade Commission (USA) collaborates with developers to establish optimal strategies for implementing safeguards and technical measures that ensure the protection of children from potential harm in immersive experiences, in addition to offering explicit guidance on COPPA compliance for AR/VR. The implementation of these optimal methods has the potential to guide any prospective modifications to the COPPA policies.

3.3.5.4. DEVELOPING REGULATIONS TO MITIGATE POTENTIAL RISKS

The extant regulatory framework governing AR/VR not only imposes superfluous limitations on these technologies, but also exhibits conspicuous deficiencies in safeguarding against possible immediate detriments. In the present paper, the researcher has expounded upon the potential privacy hazards posed by the data collected by AR/VR devices through various sensors such as eye and motion tracking. This data, whether in its raw observed metadata form or inferred computed data, may give rise to privacy concerns. In addition to its primary function of biometric identification, it possesses several secondary utilities and can be employed to deduce noteworthy personal and identifying particulars pertaining to its users. However, the current definitions of personal and biometric data fail to consider the extensive gathering and manipulation of biometric data beyond the scope of identification.[289] The potential consequences of this situation include the risk of users being subjected to various forms of harm resulting from unauthorized access or malicious exploitation of data that is not currently covered by established definitions. This could include the generation of computed psychographic data that could be used to deduce sensitive personal information. It is

[289] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 18 June 2023.

recommended that policymakers formulate a precise delineation of personal and identifying information, encompassing extremely sensitive biometric data and essential applications beyond user authentication. This approach would foster heightened safeguarding of such data while also facilitating diverse utilization scenarios. It is recommended that not only the biometric data that is observed but also the potential for manipulation of this data to reveal supplementary information about a user be taken into consideration. It is of significance that regulations concerning biometric and biometrically derived data ought not to prohibit its acquisition in a straightforward manner. The functionality of devices and applications may necessitate distinct levels of information. The acquisition of accurate computed data pertaining to a user's reactions and preferences through gaze tracking may be deemed superfluous in the context of a social experience. However, this identical data may be deemed indispensable in a market research setting. Despite its limited usage, BCI data poses analogous definitional challenges. It is premature to implement any form of direct regulation on BCI technologies. However, policymakers should exercise caution in determining the classification of both observed BCI inputs and inferred computed data from BCI-enabled devices. For privacy regulations to be effective, it is imperative that they incorporate precise delineations of biometric identifying and biometrically derived data. Additionally, these regulations should mandate transparency, consent, and choice requirements that align with the specific objectives of data collection and the potential risks of harm. Although both biometric identifying data, such as facial recognition, and biometrically derived information, such as inferred data about personal preferences from eye-tracking or BCI technologies, may be classified as personal information, they necessitate distinct protective measures. The differentiation between the entities will guarantee the provision of sufficient protection to users against any potential harm, while simultaneously enabling the exploration of novel applications of this data, subject to appropriate levels of user disclosure and autonomy.

Moreover, it is imperative to establish unambiguous protocols for the utilization of AR and VR data in legal inquiries. The comprehensive profile of an individual that can be formed by the data collected from AR/VR devices and applications renders it a potentially valuable tool for law enforcement and legal proceedings. The current legal precedent regarding digital information suggests that utilizing such data may potentially infringe upon the Fourth Amendment protections afforded to individuals in the United States. Immersive experiences have the potential to introduce a novel dimension of law enforcement application, namely, the utilization of real-time virtual presence. The emergence of multiuser AR/VR platforms has

prompted inquiries into the applicability of legal frameworks, such as the third-party doctrine, to investigators or law enforcement officials who engage with, monitor, and document the actions of users within virtual environments that are either fully or partially simulated. It is recommended that policymakers implement novel legal measures to ensure the protection of comprehensive user data in AR/VR. This may include the establishment of unambiguous directives outlining the circumstances under which access to such information would necessitate a warrant.

3.3.5.5. IMPLEMENTATION OF NATIONAL PRIVACY LEGISLATION TO HARMONIZE COMPLIANCE REQUIREMENTS AND FACILITATE INNOVATIVE PRACTICES

The implementation of regulations and rules that cater to the distinct characteristics of user privacy in AR/VR can provide protection to users and foster innovation in the immediate future. However, the enactment of comprehensive privacy legislation at the national levels of different countries instead of separate federal laws such as seen in USA, would be more advantageous for both regulators and developers, as it would enable them to consistently enforce essential safeguards as these technologies progress. It is recommended that policymakers implement privacy legislation that outlines precise protocols for the acquisition, manipulation, and dissemination of diverse forms of data, while considering the varying degrees of sensitivity involved. Additionally, such legislation should incorporate measures to protect user data privacy rights and mitigate potential risks of harm. It also enhances the efficacy of notification, transparency, and consent protocols to enable users to make well-informed decisions regarding the data they opt to disclose, encompassing delicate biometric and biometrically derived data. The process of regulatory harmonization ought to consider privacy regulations that are specific to sectors and purposes, such as HIPAA and FERPA. The implementation of regulations may introduce supplementary and possibly contradictory obligations on AR/VR technologies, which may hinder their capacity to be employed in domains where they could provide substantial benefits, such as healthcare and education. It is recommended that regulators maintain consistency in the requirements across regulations that are specific to different sectors. Additionally, any specific requirements should complement and not conflict or complicate the broader federal privacy legislation. This approach has the potential to reconcile compliance requirements that may be in conflict and establish unambiguous guidelines for safeguarding user privacy in relation to both current and emerging data collection methods in AR/VR.

3.3.5.6. ENDORSEMENT OF VOLUNTARY MEASURES TO SAFEGUARD USER PRIVACY IN VIRTUAL SPACE

Given the absence of a comprehensive federal privacy legislations as can be seen in the USA, it is crucial for developers and policymakers of Immersive Technologies to work together in order to establish an effective self-regulatory strategy which can protect the privacy of users. The implementation of clear and consistent standards and protocols will enable the tech companies associated with Immersive technologies to ensure that their products include appropriate safety measures, while also providing legislators and regulatory bodies with a more thorough understanding of the most effective and technically feasible risk reduction methods. It is advisable for federal entities (in USA), including the Departments of Education (USA), Health and Human Services (USA), and Transportation (USA), to engage in joint efforts with AR/VR developers to devise voluntary protocols for protecting user privacy in AR/VR, while considering relevant circumstances. It is advisable to establish a framework for AR/VR technologies that is grounded in established standards and best practices, while also considering the unique or heightened risks and potential for harm that these technologies may present. It is imperative to acknowledge that the integration of voluntary standards for AR/VR necessitates the participation of developers from diverse sectors and industries, including but not limited to education, healthcare, entertainment, and workforce development. There are a multitude of existing contributions within this field that can potentially serve as a basis for a framework specifically designed for AR/VR. Notable examples of privacy-focused initiatives in the XR industry are the Privacy Framework established by the XR Safety Initiative, the Privacy Manifesto put forth by the Open AR Cloud, and the Developers Guides series published by the XR Association.[290] The establishment of industry-specific standards is necessary due to the vast amount of data collected by AR/VR devices and applications, despite the foundational framework provided by the NIST Privacy Framework.[291] The aforementioned refers to the previously mentioned information or ideas. The incorporation of transparency and disclosure

[290] 'XRSI Privacy Framework Version 10' (*XRSI,* September 2020) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 19 June 2023; Jan-Erik Vinje, 'Privacy Manifesto for AR Cloud Solutions' (*Open AR Cloud on Medium,* 17 October 2018) <https://mediumcom/openarcloud/privacy-manifesto-for-ar-cloud-solutions-9507543f50b6> accessed 19 June 2023; XR Association, 'Research & Best Practices' (*xraorg,* 10 Febraury 2021) <https://xraorg/research-best-practices> accessed 19 June 2023.

[291] National Institute of Standards and Technology, 'NIST Privacy Framework' (*US Department of Commerce National Institute of Standards and Technology,* 16 January 2020) <https://wwwnist.gov/system/files/documents/2020/01/16/NIST Privacy Framework_V1.0.pdf> accessed 19 June 2023.

protocols and mechanisms is of paramount importance for immersive experiences, particularly with respect to furnishing lucid disclosure regarding the gathering and application of sensitive biometric data. Furthermore, it is recommended to establish user privacy controls and opt-out mechanisms for non-essential information. It is imperative to maintain information security standards, which entails ensuring the encryption and local storage of extremely sensitive data, such as biometric identifiers or spatial mapping of private residences. Moreover, it is imperative to establish protocols for the acquisition and utilization of biometrically derived data for objectives beyond user authentication. The establishment of standards has the potential to identify areas where policy intervention may be necessary to ensure comprehensive protection of users from harm. This may encompass the enactment of legal measures that pertain to matters concerning infringements upon individual autonomy and instances of discriminatory conduct.

CHAPTER 4

IMMERSIVE TECHNOLOGY- A WAY FORWARD

4.1. INTRODUCTION

In the upcoming generation of immersive media, it is plausible that standard features in VR and AR systems will include advanced hand, limb, and eye tracking, haptic or neurological interfaces, and pupil dilation hardware. The company Oculus has made an official announcement regarding the implementation of hand tracking technology, which aims to eliminate the requirement for controllers. Hand tracking was introduced on Oculus Quest devices in December 2019,[292] thereby obviating the necessity for controllers. The functionality of this characteristic is dependent upon the utilization of hand scans, in conjunction with anticipatory artificial intelligence derived from neural networks, to generate a 3D representation of the hand within a virtual environment.[293]

Several corporations are taking a step further by utilizing brain waves to operate computer devices. They have showcased models of neural link sensors that eradicate the necessity of physical gestures. During the Slush event in November 2019, Next Mind, a company, presented a real-time demonstration of a non-invasive brain-computer interface.[294] The event was a significant start-up conference held in Finland. The apparatus is positioned at the posterior region of the user's cranium, and expeditiously deciphers neural impulses originating from their visual cortex, subsequently converting them into digital directives that can be instantaneously executed by any compatible device.[295] During the presentation, the individual exhibited their ability to manipulate the motion of a cursor by means of their cognitive processes, facilitated by a sensor affixed to their cranium and integrated with a virtual reality head-mounted display.

Certain advancements have proven to be exceptionally advantageous for communities that have historically been excluded or have disabilities. The proposal under consideration is the

[292] Meta Quest, 'Oculus Connect 6: Introducing Hand Tracking on Oculus Quest, Facebook Horizon and More' (*Meta,* 25 September 2023) < https://about.fb.com/news/2019/09/introducing-hand-tracking-on-oculus-quest-facebook-horizon-and-more/> accessed 20 June 2023.
[293] 'Using deep neural networks for accurate hand-tracking on Oculus Quest' (*Meta,* 25 September 2019) <https://bit.ly/2ZoQVHw> accessed 20 June 2023.
[294] 'NextMind Unveils World's First Brain-Sensing Wearable That Delivers Real-Time Device Control with Just Your Thoughts' (*Businesswire,* 21 November 2019) <https://www.businesswire.com/news/home/20191121005757/en/NextMind-Unveils-Worlds-First-Brain-Sensing-Wearable-That-Delivers-Real-Time-Device-Control-With-Just-Your-Thoughts> accessed 20 June 2023.
[295] Ibid.

development of a haptic shirt that enables individuals with hearing impairments to perceive various musical instruments through tactile sensations, thereby providing them with a novel musical experience. Consider the scholarly endeavors of Dr. David Eagleman, who employs technical interfaces to generate novel sensory experiences for individuals with disabilities. Although the integration of his haptic vest with immersive technology is not explicitly addressed, it is conceivable that such integration could be a potential application, particularly in the context of gaming or romantic experiences.[296] The utilization of haptic gloves in virtual experiences has the potential to expand the scope of verisimilitude. The utilization of pupil dilation is currently being developed for immersive therapies related to mindfulness, with the aim of utilizing this technique to map the unique cognitive landscape of individuals as a means of promoting healing. Companies such as Tripp are utilizing immersive technology to leverage its potential for therapeutic and wellness applications.[297]

The impetus behind innovation may stem from a desire to enhance user experiences and customize products. However, this may engender a precarious situation with regards to safeguarding privacy and upholding human rights.

4.2. THE CURRENT LEGAL SCENARIO

The current legal framework fails to accommodate emerging paradigms in immersive technology. The emergence of new technology has raised several inquiries that surpass the existing legal boundaries. What is the methodology for collecting scans of user data? What is the mechanism of information storage? What is the frequency of information updates? What is the duration of data retention? What criteria would a court employ to distinguish between a solitary image and a continuous flow of data? Can the longitudinal monitoring of muscular activity be classified as an aspect of facial geometry, as delineated in the biometric regulations mentioned earlier? Do these applications have constraints solely within the realm of identity or do they represent an extension of the underlying notion?

As technological advancements progress, additional gaps and ambiguities in legal frameworks may become apparent. Physiological attributes pertaining to movement may fall beyond the scope of authorized classifications of biometric data or biometric identifiers. One potential application is gait tracking, which involves the identification of individuals within a crowd

[296] Jeremy Hsu, 'Real "Westworld" Haptic Vests Better Than Fiction' (*Discover Magazine*, 8 June 2018) <https://www.discovermagazine.com/technology/real-westworld-haptic-vests-better-than-fiction> accessed 24 June 2023

[297]TRIPP: Fitness for your Inner Self, TRIPP, <https://www.tripp.com/> accessed 24 June 2023.

based on their unique walking patterns. Due to the unique characteristics of an individual's bone structure and movement patterns, the way they tilt their head while utilizing a VR or AR headset, as well as the quality of their gestures within an immersive environment, can be equally distinctive in identifying an individual as their fingerprints, retinas, or vocal patterns.[298] The integration of data sets and the creation of distinct identifiers were not envisioned during the drafting of the statutes.[299]

Consumer-based headsets for VR and AR lack the capability to track all the characteristics. The investigation has predominantly been limited to controlled laboratory and research settings, or customized applications tailored to specific clients. Police departments in China utilize AR overlays to implement facial recognition technology on large groups of people, thereby enabling the identification of potential suspects.[300] The United States military is currently in the process of developing interfaces that utilize AR technology to aid in the identification and targeting of adversaries, whether in a combat situation or within a civilian population. Military entities are currently conducting trials of facial recognition technology within augmented reality interfaces.[301]

The trend towards consumer adoption is expected to involve the integration of location-based advertising models and the monetization of user data to external entities. As a result, it is plausible that corporations will increasingly introduce functionalities to explore the physiological and psychological conditions of their users, thereby generating a need for biometric psychographics. Enhancing advertisers' knowledge about their intended audience, such as their level of attentiveness, emotional response to product interaction, and personal health and well-being characteristics, can potentially increase the likelihood of converting them into a more receptive customer base. It is imperative to consider the need for augmentations or supplements to the existing legal framework, alongside the elucidation of current statutes, with the aim of safeguarding the fundamental right to privacy.

[298] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 24 June 2023.
[299] Ibid.
[300] Josh Chin, 'Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal' (*The Wall Street Journal,* 7 February 2018) <https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353.> accessed 24 June 2023.
[301] Al Restar, 'US Army Is Testing Facial Recognition Goggles' (*Z6 MAG,* 22 July 2019) <https://z6mag.com/2019/07/22/us-army-is-testing-facial-recognition-goggles/> accessed 24 June 2023.

4.3. IMPLICATIONS OF BIOMETRIC PSYCHOGRAPHY ON HUMAN RIGHTS

As we have already discussed in earlier chapters about the term 'Biometric Psychography' coined by Brittan Heller in her research work 'Reimaging Reality' about the challenges associated with it regards to privacy. Let us now discuss about the potential implications of its usage on the Human Rights of the users of immersive technology.

The amalgamation of data sets inherent in immersive technology has the potential to yield additional intrusive outcomes for users that surpass mere infringement of consumer privacy. As aforementioned, the diagnostic value of measuring eye movement in conjunction with pupil response has already been established. The extent to which eye movements can unveil information is often a source of astonishment for individuals. For instance, scrutinizing saccades, the rapid and jerky eye movements that enable us to form a visual representation of our surroundings, or the "smooth pursuit" movements that the eye executes when tracking a mobile object can yield valuable insights.[302] Certain scholars have discovered that atypical eye movement patterns may serve as an indicator of autism in certain young children. Eye tracking has the potential to diagnose various severe medical conditions, including but not limited to schizophrenia, Parkinson's disease, ADHD, and concussions.[303]

This has the potential to have significant consequences. A study was conducted by German scientists wherein participants were tasked with navigating a VR maze. The study revealed a significant correlation between users' task performance and their ability to predict their susceptibility to developing Alzheimer's disease.[304] The correlation between an individual's medical health and their performance on a VR game was likely not foreseen by the creators of health privacy laws. The potential availability of such data for purchase by third-party entities, such as insurers, is a matter of concern.

As previously discussed, the measurement of pupil dilation has the potential to reveal highly personal information, such as an individual's inner thoughts and desires. It is disconcerting to consider the possibility of companies utilizing personal information, such as an individual's probable sexual orientation, to enhance their current commercial profiles. The possibility of

[302] Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail' (*Vice*, 28 May 2019) <https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 24 June 2023.

[303]Ibid. Tia Ghose, 'Eye Tracking Could Diagnose Brain Disorders' (*Live Science*, 18 September 2012) <https://www.livescience.com/23274-eye-tracking-gazebrain-disorders.html> accessed 24 June 2023.

[304]David Schultz, 'Alzheimer's disease tied to brain's navigation network' (*Science*, 22 October 2015) <https://www.sciencemag.org/news/2015/10/alzheimers-disease-tied-brain-s-navigation-network> accessed 24 June 2023.

censorship in its most fundamental form arises when users attempt to restrict their thoughts, feelings, or expressions, particularly if such information can be monetized or researched. Simultaneously, a considerable number of these factors are subliminal, implying that the user's inclination to self-censor or conceal their predilections is rendered impracticable.

If third-party or direct developers possess the capability to integrate disparate data sets in manners that are unforeseen or detrimental to consumers, it may lead to the disclosure of information that users did not intend to reveal or provide meaningful consent for. In the absence of standardized legal regulations or self-imposed limitations beyond the realm of identifying data, as emphasized in contemporary biometric systems, corporations may be vulnerable to a similar large-scale breach of user confidence akin to that of Cambridge Analytica. Educating users about the extensive ramifications of data collection can be a complex task, as many individuals lack comprehension of how involuntary physiological cues, such as emotional responses, mental state, or health indicators, can reveal deeply personal information, including but not limited to truthfulness, inner emotions, and sexual arousal. The potential effects of recently introduced state-level privacy regulations, such as the CCPA, on consumers and immersive technologies are yet to be fully understood. Specifically, the voluntary option restricting data selling by consumers may have implications for the evolving data sets and personal information associated with immersive technologies, which are becoming increasingly popular.

4.4. VULNERABILITIES AND EXPERIENCES IN IMMERSIVE TECHNOLOGY

The utilization of immersive technology's biometric richness poses a noteworthy security threat in terms of user privacy, health, and safety. Advocates have not yet made cybersecurity concerns for immersive hardware a mainstream issue. Upon contemplation of the attributes such as character, quality, and quantity of information that can be perceived through a VR encounter, it is probable that a cybercriminal would perceive the immersive hardware as a lucrative source of information.

Tom Furness expresses concern regarding the potential weaponization of VR/AR hardware if a malicious agent was to intentionally cause harm to users. In essence, the utilization of an HMD necessitates the coordinated operation of both monocular and binocular vision in order to enable the eye to achieve focus on an object that is proximal in nature but appears to be distal. Inadequate execution of the task may result in a prolonged impairment or even complete

loss of vision for several months.[305] In the event of hardware susceptibility to hacking, it is plausible for a malicious individual to manipulate a headset with the intention of deliberately impairing a user's vision. The potential hazards associated with these systems, which are heavily reliant on bodily functions and physiology, transcend beyond matters of confidentiality.

Additional scholars have identified possible susceptibilities in VR/AR material that may result in negative consequences for individuals. Potential examples of unethical behavior in virtual environments may encompass a range of actions, such as the intentional manipulation of AR directions to deceive or endanger users, the misrepresentation of one's identity within VR spaces, the theft of virtual goods within gaming contexts, the act of virtually impersonating others, or the addition or removal of content in a manner that may elicit fear or shock in users, potentially leading to physical ramifications.[306] Insufficient safeguarding of the authenticity of software or user interactions may lead to the inappropriate exploitation and manipulation of programming.

Certain hardware vendors are developing biometric systems as a more secure substitute for passwords. The HoloLens2 developed by Microsoft generates a digital signature by utilizing the Iris-ID. However, proponents caution against the possible instability that may arise from linking such immutable data with online accounts in the event of a security breach. If the present ocular signature corresponds to the previously recorded signatures, then the individual in question can be identified as themselves. On the premise that one's iris signature is distinct and remains secure, it is superior to passwords. The optimal security measure entails the storage of said signatures on the device, within a hardware-based encrypted repository. The theft and decryption of a physical device by a resolute hacker would likely entail a protracted and arduous endeavor. This phenomenon renders the execution of exploits, particularly those that target many systems, a more challenging task. The act of transferring this data to the cloud has the potential to enhance user convenience through various means such as system backup and restoration, as well as facilitating cross-device logins. The act of obtaining an individual's signature and subsequently "replaying" it in their absence has the potential to facilitate impersonation, thereby posing a threat to the individual's security. The process of resetting

[305] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf > accessed 25 June 2023.
[306] Mark Lemley & Eugene Volokh, 'Law, Virtual Reality, and Augmented Reality' (2018) 166 University of Pennsylvania Law Review 28-29.

passwords is a straightforward task. Modifying one's ocular features can be a challenging task. A single instance of breach can have long-lasting and detrimental effects.[307]

The integration of immersive technologies with public authority poses heightened vulnerabilities for hacking. As noted earlier, Chinese law enforcement agencies utilize AR overlays to implement facial recognition technology in order to identify suspects within crowds, while military organizations[308] are also in the process of creating augmented reality interfaces to target adversaries both on the battlefield and within crowds.[309] The utilization of immersive technology in defense applications may pose a potential risk of hacking, which could result in the misidentification of friendly targets or allies.

4.5. HUMANITARIAN SOLUTION TO HUMAN RIGHTS ISSUES IN IMMERSIVE TECHNOLOGY

Considering the risks associated with immersive technologies, what proactive measures can be taken by companies, experience developers, regulators, and legislators to alleviate any potential negative human rights consequences stemming from the use of AR and VR?

4.5.1. ESTABLISHING VALUE-BASED HEURISTICS AND ENSURING THAT EXPERIENCE RULES ARE CLEARLY UNDERSTOOD BY USERS

The creation of virtual spaces has the potential to facilitate novel social experiences, as it allows for the representation of non-living entities, the construction of novel environments, the manipulation of physical laws and natural phenomena, and the embodiment of diverse physical forms. Nonetheless, a limited number of individuals possess knowledge regarding the social norms that are relevant when engaging with an individual who may seem to resemble a conversing with a kitchen appliance.

The lack of inter-platform operability remains an unresolved concern within the nascent VR/AR industry. As various HMDs and systems continue to advance, users will inevitably develop unique gestural patterns, modes of interaction, and spatial navigation techniques that are closely linked to the specific immersive experiences they are engaged in, as well as the

[307]Avi Bar-Zeev, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail' (*Vice*, 28 May 2019) <https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 25 June 2023.
[308]Josh Chin, 'Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal' (*The Wall Street Journal*, 7 February 2018) < https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353> accessed 25 June 2023.
[309]Al Restar, 'US Army Is Testing Facial Recognition Goggles' (*Z6 MAG*, 22 July 2019) <https://z6mag.com/2019/07/22/us-army-is-testing-facial-recognition-goggles/> accessed 25 June 2023.

technical constraints of the platforms that support them. For example, the VR game Beat Saber which has gained significant popularity and commercial success. The game involves the player slicing blocks that are propelled towards them using light sabers, all while keeping in time with a musical soundtrack. The Oculus Quest offers the option of accessing the available formats of Beat Saber in either 90 or 360 degrees. Nonetheless, individuals utilizing the PSVR platform will discover that Beat Saber solely exists in its initial head-on configuration and is not subject to any updates. Drawing from the technical constraints inherent to the PSVR system. An additional instance that can be anticipated, wherein technical specifications have an impact on and alter user interaction, is the implementation of foveated rendering on VR systems. This can condition users to adopt specific behaviors, such as directing their gaze towards their area of interest to obtain a more intricate view. The obstacles posed by technological constraints in shaping interactivity bear resemblance to those encountered when dealing with multiple iterations of identical immersive experiences. Divergent circumstances between Oculus and PSVR users will likely result in disparate approaches to engaging with Beat Saber, consequently leading to distinct modes of interpersonal communication. The phenomenon is commonplace in emerging industries; however, it poses a significant obstacle in the realm of immersive media. This is due to a discrepancy between established communication strategies and prevalent cognitive frameworks utilized for interpreting said communication. The evaluation of potential risks to user safety and human rights in product design necessitates the consideration of technical-social aspects.

Such behavioural codes which emerge in immersive ecosystems may not be transferrable, thereby presenting a challenge to users who seek to comprehend the meaning of communications in a new social setting. The establishment of a shared language and tangible set of guidelines for engaging in virtual environments, which accounts for the diverse range of anticipated conduct, interactive features, and implicit conventions of the space, can effectively curtail detrimental actions. There are two methods by which this task can be accomplished. Initially, it is noteworthy that social media has addressed the issue of fluctuating social norms and unstable connotations through the implementation of communal moderation remedies.[310] Dr. J. Nathan Matias has conducted scientific research on the efficacy of community-based moderation on the social media platform Reddit. His research highlights the potential of this approach as a more adaptable, influential, and feasible alternative to content moderation systems that are centralized and hierarchical in nature. Furthermore, it is possible for both

[310] Dr. J. Nathan Matias, J. NATHAN MATIAS, <https://natematias.com/> accessed 25 June 2023.

hardware system developers and creators of immersive content to establish unambiguous user behavioural expectations through platform onboarding experiences. The initial programming experience frequently serves as the user's initial exposure to a virtual environment, and can significantly shape their behavioural expectations and anticipated interactions with others.

The process of level setting can manifest in various ways, and designers are tasked with the decision of whether to impose penalties on users who deviate from desired behavioural norms, offer positive reinforcement to those who exhibit pro-social behaviours, or incorporate a combination of both strategies. Irrespective of the situation, it is crucial to prioritize clarity. An illustration of this can be seen in the former Facebook Spaces, where users were presented with guidelines for behaviour upon entering a new social environment. Specifically, the guidelines emphasized the importance of being hospitable, stating: "Be Welcoming, be respectful and be kind."[311] The act of reminding users that there is a human being on the receiving end of their virtual experience can significantly influence cultural norms and adjust user expectations regarding acceptable behaviour in online environments.

Empirical studies conducted on social media platforms have demonstrated that the conspicuous presentation of regulations for users, coupled with explicit communication of anticipated standards for constructive user conduct, can serve as a preventive measure against minor misconduct and unintentional negative consequences. The findings of a research conducted on the issue of abuse in Reddit forum indicate that the prominent display of rules in a concise and easily comprehensible format increases the likelihood of adherence to these rules, thereby significantly reducing the incidence of inadvertent or negligent violations.[312] Drawing from these valuable insights, Twitter undertook a comprehensive revision of its community standards, aiming to condense the rules into concise missives that can be displayed conspicuously. It is a justifiable proposition that imparting the regulations governing virtual encounters in a succinct, lucid, persuasive, and accessible manner would yield comparable outcomes.

[311] Michelle Cortese & Andrea Zeller, 'How to protect users from harassment in social VR spaces' (*The Next Web,* 2 January 2020) <https://thenextweb.com/syndication/2020/01/02/how-to-protect-users-from-harassment-in-social-vr-spaces/> accessed 25 June 2023.
[312] J. Nathan Matias, 'Posting Rules in Online Science Discussions Prevents Problems & Increases Participation' (*Civilservant,* April 2019) <http://civilservant.io/r_science_sticky_coments_1.html> accessed 25 June 2023.

4.5.2. DIFFERENT LEVELS OF IDENTIFICATION WITHIN CONTENT MODERATION LAYERS IN THE VIRTUAL SPACE

As aforementioned, individuals involved in the design of virtual environments must possess an understanding of the various tiers at which content moderation can be implemented within an immersive system. The three layers of the immersive platform are the content layer, the behavioural layer, and the account layer. The content layer is responsible for providing individual immersive experiences like software. The behavioural layer facilitates user-to-user interactions and interactivity between users and the environment. Lastly, the account layer is where users register and access features of the immersive platform. Considering the existence of the layers, what form of content moderation would be appropriate for virtual environments?

The navigational complexity of the behavioural layer is notably high, owing to the presence of numerous actors and factors, as well as its direct association with the freedom of expression. Initial experiments conducted on social VR platforms involving live moderators have revealed that their effectiveness was limited, as their presence was akin to that of a middle school hall monitor. Consequently, instances of misbehaviour either persisted or escalated once the moderator was no longer present.[313] A further challenge pertains to the appropriate role of moderators in public VR environments that feature private rooms with an expectation of privacy. Online platforms need to find a way to implement live moderation without creating an atmosphere that resembles a surveillance state, which could potentially violate the privacy of users. At the same time, they must ensure that their platforms do not become a breeding ground for abusive behaviour.

It is plausible to align social norms more closely with those observed in physical settings, about the emulation of socially acceptable conduct. Nonetheless, it must be acknowledged that there are inherent deficiencies in the efficacy of current social norms. This is a sentiment that is likely shared by numerous individuals from marginalised communities who perceive offline norms to be inadequate. Individuals belonging to certain demographics who encounter harassment in real-life settings may be disinclined to witness the validation of abusive or harassing conduct in novel virtual domains.

[313] Taylor Lorenz, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here is Why I Keep Going Back' (*Mic, 26 May 2016*) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> accessed 26 June 2023.

A potential alternative perspective on content moderation could involve a community-oriented approach that prioritises values, with the aim of strengthening social bonds. This approach may also involve the integration of multiple groups to mitigate the effects of filter bubbles. Studies conducted by experts in the field of online behavioural interaction have revealed that community-based moderation systems have demonstrated a certain level of effectiveness. This can be attributed to their ability to tailor regulations to suit the specific needs of the forum, the expectations of users, and the evolving preferences of the community. The efficacy of community-based moderation on Reddit has been the subject of scientific research conducted by Dr. J. Nathan Matias.[314] His extensive body of work highlights the potential of this approach as a more adaptable, influential, and feasible alternative to content moderation systems that are centralized and hierarchical in nature.

In the context of account layer, content moderation and online harassment may exhibit dissimilar characteristics due to the varying risk profile associated with distinct types of information in the stack. It is imperative for companies that offer immersive experiences to acknowledge the inherent risks associated with their hardware and software and implement optimal measures to mitigate cybersecurity risks. One potential measure is to require external security audits of hardware conducted by experts, with a focus on safeguarding privacy, enhancing security, and promoting user safety.

The application of audits could extend to the evaluation of immersive content for redlining. Consider the potential hazards associated with experience-driven virtual economies, wherein users can procure upgrades and supplementary functionalities to augment their engagement with other users and the all-encompassing infrastructure. The VR game's marketplace has the potential to encompass personal details such as geographical positioning, media consumption patterns, and communication dynamics, including the identity of the individuals involved and the nature of their interactions. In addition, the bundling of financial information with a user's data may occur due to intra-experience transactions and game subscriptions. In order to safeguard susceptible users and demographics, it is imperative for companies to scrutinise the strategic susceptibilities inherent in the features of immersive experiences, like their approach in other online environments. Potential security risks may arise from various factors such as widespread usage of screennames, which could potentially facilitate password hacking, or the utilisation of names and locations for the purposes of phishing and social engineering.

[314] J. Nathan Matias, 'Posting Rules in Online Science Discussions Prevents Problems & Increases Participation' (*Civilservant*, April 2019) <http://civilservant.io/r_science_sticky_coments_1.html> accessed 26 June 2023.

Furthermore, it is advisable for companies to assess the security records and practises of third-party content providers such as Steam or other external content marketplaces. This includes evaluating their breach notification and response mechanisms, malware protection measures, and availability of multi-factor authentication. This precautionary measure is necessary to prevent the inadvertent introduction of security vulnerabilities into the company's systems. In general, it is advisable for companies to address any vulnerabilities promptly and comprehensively in their infrastructures and applications, regardless of whether they are immersive in nature.

4.5.3. IMPLEMENTING A RATING-BASED SYSTEM FOR ENTERTAINMENT IN DIGITAL SPACE

An additional proposal, beyond the realm of hardware, would entail exploring interventions that impact social systems beyond user conduct, with a focus on enhancing the immersive experiences per se. Various forms of media, such as video games, music, and motion pictures, have implemented rating systems to assist consumers in making informed choices regarding the material they wish to access, whether for themselves or their children. Certain rating systems categorise various forms of media into age-appropriate classifications. Although it may not completely mitigate the potential adverse effects of user misconduct or eliminate the possibility of encountering explicit content, such as violent imagery, it would furnish users with the necessary information to make informed decisions regarding their participation in immersive experiences. This proposed scheme would enable users to engage in more informed, intentional, and consensual interactions with VR experiences. This holds significant importance, given the characteristics of immersive experiences that engender a sense of realism and embed themselves in our psyche as memories.

4.5.4. PROTECTION OF PRIVACY BY GIVING CONTROL WITHIN VIRTUAL SPACES OVER THE COLLECTION OF DATA AND STORAGE OF DATA

A VR interface can be defined as a HMD equipped with six cameras. The integration of additional sensors into the HMD raises complex inquiries regarding the storage of data that are likely to persist. Is there a provision for users to opt out of remote data transmission or storage by the headsets? Can this be considered a feasible alternative, considering the substantial volume of data produced by immersive experiences and the industry's objective of achieving platform interoperability? What are the complications posed by the interactivity between MR browsers and HMDs?

It is imperative to assess the applicability of pre-existing data regulations in immersive environments, particularly considering the hazards associated with networked data and the potential for physical and psychological consequences arising from immersive technologies. Moreover, with regards to anticipated legal advancements, there exists a significant likelihood of conflict of laws due to the limited number of states that have enacted biometric legislation.

One potential framework for addressing these challenges involves examining the incremental development of legislation pertaining to online harassment, which has been characterised by several obstacles and challenges. Initially, initial endeavours to address harassment revealed a fundamental deficiency in comprehension, as certain lawmakers appended the terms “cyber” or “online” to pre-existing statutes in manners that were incongruous with the operational mechanisms of the technology. An instance could be a harassment statute that is limited to the state level and mandates that the abusive conduct must be explicitly conveyed between the victim and the offender, thereby rendering it inapplicable to certain types of digital interactions.[315]

Authentic informed consent necessitates a degree of comprehensive comprehension by individuals regarding the methods through which their data is being gathered, utilised, retained, and traded. Furthermore, it is recommended that users are granted autonomy in determining the way these procedures take place, with the default option being opt-out rather than opt-in.

In conclusion, the practise of data localization is highly recommended as a best practise. Ideally, sensitive user data should be retained within the HMD rather than being transmitted, stored, or preserved on external servers. Thus, it is possible to collect or store highly confidential data and utilise it to enhance the user's experience, all while ensuring that the user retains sole ownership of said data and that it is not shared with any external entities. In exceptional circumstances, it may be feasible for authorities to obtain access to the information, albeit with considerable difficulty, and typically within the confines of legal regulations.

[315] Danielle Citron, *Hate Crimes in Cyberspace* (1st edn, HUP 2014).

4.5.5. CREATING INDUSTRY-WIDE CODES OF CONDUCT[316]

Given the current state of flux in immersive interfaces and the ongoing evolution of the industry, it would be a precarious endeavour to draft legislation aimed at addressing forms of harm. Nevertheless, it is not to be assumed that a future law on it is not a viable proposition. During the transitional period, it is recommended that measures such as codes of conduct, limitations, along with thorough scrutiny of the fundamental aspects of immersive technologies be implemented in order to mitigate potential negative consequences.

Immersive technologies ought to strive for superior performance compared to internet-based platforms, thereby presenting an opening to avoid replicating certain fundamental errors of online media. Fortuitously, there is an existing framework that can aid. The UNDPs provide companies with a framework to ascertain their responsibility in advancing and executing human rights.[317] The Ruggie Principles, otherwise referred to as the UNDPs, advocate for a comprehensive structure that mandates governments to safeguard human rights, corporations to uphold human rights, and both entities to ensure redressal mechanisms are in place in the event of human rights violations. Industries which are characterised by elevated levels of operational risk, such as oil, gas, mining, and nuclear, have collaborated to establish these codes of conduct. The ability of entities to govern themselves enables them to exchange optimal methodologies, collaboratively pre-empt negative consequences and offer solutions, and mitigate mutual hazards that pervade the sector. Hence, it is advisable for companies that offer immersive experiences to assess the compatibility of their modus operandi with the UNDPs guidelines. This evaluation should be integrated into their fundamental business practises during the early stages of their development.

The initial phase towards adherence to the UNDPs involves an examination of the overarching principles that intersect within a given sector, followed by the establishment of a mutually agreed-upon accord among relevant parties. At present, there exists no established set of ethical guidelines or standards of behaviour for the immersive industry. Considering the extensive and diverse range of potential negative consequences for users, taking a proactive approach would be beneficial in enabling companies to anticipate and effectively address challenges. This would also enable users to ensure that adequate measures are in place to combat potential

[316] UN Human Rights Council, Protect, respect and remedy : a framework for business and human rights : report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, 7 April 2008, A/HRC/8/5, <https://www.refworld.org/docid/484d2d5f2.html> accessed 30 June 2023.
[317] Ibid.

adverse effects. By adopting this approach, it is possible to guarantee that the incorporation of human rights principles can play a constructive part in the foundational operations of emerging enterprises and technological frameworks.

CHAPTER 5

CONCLUSION AND SUGGESTIONS

5.1. FINDINGS

The present analysis aims to examine the outcomes of each chapter in a sequential manner, with the ultimate objective of deriving the overarching findings of the research on the Influence of Immersive Technologies on the Human Rights of their users, with a particular focus on the aspects of Privacy and Data Protection.

The article highlights the prospective transformative impacts of the metaverse on the interplay between humans and technology, as well as on the broader association between humans and their environment. The term "metaverse," which refers to a digital realm, is currently in its beta stage and its final configuration has yet to be fully established. The current state of the metaverse can be likened to rudimentary constituent components, and the precise arrangement of the metaverse, as depicted in the literary and cinematic oeuvre of Ready Player One (OASIS), is currently in the process of being constructed. Additionally, our study suggests that the present availability of the metaverse is limited owing to the inadequate development of a digital ecosystem. However, notable technology corporations have commenced the creation of their proprietary hardware to facilitate the attainment of immersive experiences. Notable examples include Facebook's acquisition of Oculus and Apple's recent introduction of their own virtual reality headsets. The emergence of hardware by private entities has given rise to apprehensions regarding the acquisition of complex and constantly evolving user data by these firms and corporations, thereby exposing users to the consequences of surveillance capitalism. Additionally, it has been observed that the ownership of the metaverse remains undetermined, prompting numerous large technology firms and corporations to act to monopolize and gain a first-mover advantage in the metaverse economy through the utilization of technological advantages and intellectual property rights. As previously mentioned in the discourse on metaverse regulation, the researcher concludes that in order to mitigate the exacerbation of pre-existing internet risks or the emergence of new ones, it is crucial for digital regulation to become more flexible and forward-thinking in relation to the metaverse. The research indicates that effective regulation of the metaverse necessitates collaboration among international and national regulatory bodies, as well as major technology firms and corporations that possess extensive knowledge of immersive technologies. The participation of both international and national regulatory bodies serves to inhibit large corporations from exploiting immersive technologies and metaverse for the purpose of surveillance capitalism and commercial gain. In

addition, the participation of large firms and corporations facilitates the regulatory process for both international and national regulators, enabling them to address technical matters. Furthermore, the involvement of these entities engenders satisfaction and raises questions regarding their economic entitlements in the development of technology. It is imperative to engage in a robust discourse and exhibit a sense of apprehension regarding the prospects of a digital milieu, particularly with regards to safeguarding the privacy and data protection of individual users, and thwarting any potential infringement by corporate entities for their own economic gains.

In the subsequent chapter pertaining to Immersive Technology, the researcher has determined that the technology is currently in a nascent stage of development. Furthermore, the devices required to access this technology are also undergoing development. Most of these devices are subject to scrutiny due to their origin from large private technology firms and corporations whose primary objective is the practice of surveillance capitalism. Additionally, the study's researcher discovered numerous psychological traits linked to the utilization of Immersive technology. It was observed that the way a person’s brain recollect experience in a virtual environment is comparable to how we form memories of non-virtual or real experiences. Consequently, due to these psychological facets of immersive technologies, it is apparent that the human rights of its users are affected. Additionally, the researcher discovered in the chapter that immersive technologies possess the capability to enhance inclusivity and equity in both digital and non-digital environments. Additionally, the researcher discovered in the chapter that immersive technologies possess the capability to enhance inclusivity and equity in both digital and non-digital environments. To accomplish this objective, policymakers and regulators of immersive technologies must implement measures to address potential disparities. It is imperative that all users of immersive technology are safeguarded against potential risks and challenges. Furthermore, vulnerable users should not encounter any obstacles in utilizing such technology, nor should they be subjected to any form of bias or discrimination within the immersive technology realm.

After the present section, the succeeding chapter pertains to the topic of privacy. Within this chapter, the researcher has expounded upon the significance of the Right to Privacy and Data Protection as fundamental Human Rights, as recognized by both International Human Rights Law and National legislations, including that of India. Additionally, within this chapter, it has been discovered that immersive technology devices present new challenges regarding user privacy as a result of the varied nature of the information they gather from users. In order to address the risks associated with immersive technologies, it is recommended that regulators

and policymakers reform the current regulatory mechanisms for data privacy. This is necessary as the current system has been deemed inefficient and has failed to regulate certain risks associated with immersive technology, as discussed in Chapter 3 of the study. The researcher discovered in the chapter that data pertaining to immersive technology ought not to be regarded as a singular technology, but rather as a compilation of various technologies that collectively provide a unified experience. The collection of observables, observed, computed, and associated data encompasses various types that differ in sensitivity and potential for harm. Focusing on mitigating the tangible negative consequences rather than the technologies per se can facilitate policymakers and developers of immersive technology in distinguishing between user preferences and significant privacy hazards. Developers can directly address various forms of privacy preferences, which may require additional policy interventions to mitigate potential risks associated with user information. Additionally, the researcher has discovered that addressing the complexity surrounding user privacy in immersive technologies necessitates an equally nuanced approach to mitigate the significant threats posed by the scope and scale of data collection. Simultaneously, it is imperative to refrain from implementing regressive actions that may impede advancements in immersive technology and its various applications, as well as its novel methods of safeguarding user privacy within the digital ecosystem. The researcher concluded that policy makers can create a regulatory environment that fosters innovation in immersive technology while also establishing safety guidelines or codes of conduct within immersive environments by considering collection of different data types and adverse effects that may arise.

The study's concluding chapter revealed the potential of immersive technology, highlighting its prospects that may encompass sophisticated tracking of body movements, haptic or neurological interfaces, and pupil dilation hardware. Several prominent technology companies, including Oculus (a subsidiary of Meta), have initiated the development of hand tracking technology that aims to eliminate the need for controllers. The form of progress gives rise to the challenge of formulating 'biometric psychography',[318] which pertains to the amalgamation of behavioural and anatomical data that can be utilized to recognize or quantify an individual's response to stimuli over a period. This data can be employed to gain an understanding of an individual's physiological, psychological, and emotional condition, as well as their preferences. Therefore, the findings of the study suggest that the utilization of immersive technology by big

[318] Brittan Heller, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 Carr Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf> accessed 24 June 2023.

tech firms and corporations for eye tracking and pupil dilation monitoring can reveal information beyond identity, which has significant implications for user privacy, human rights, and the potential for self-censorship. Furthermore, it has been discovered by researchers that virtual spaces have the potential to generate novel forms of social interactions, facilitated by the capacity to anthropomorphize non-living entities, fabricate novel surroundings, manipulate the principles of physics and the natural world, and embody diverse physical configurations.

5.2. CONCLUSION

In conclusion, the researcher asserts that the emergence of Immersive Technology constitutes a noteworthy progression for humankind. It is imperative to recognize that akin to a coin, this innovation carries with it both favourable and unfavourable ramifications. Thus, it is crucial to incorporate safety protocols during the creation, implementation, and management of Immersive Technology. The consideration for human rights, including freedom of expression, safety and security, privacy, and data protection, should be regarded as a significant issue with regards to Immersive technology due to its potential impact on the physical and mental well-being of users.

International regulatory bodies and domestic lawmakers faced comparable obstacles when dealing with matters concerning the integration of online media into our societal and legal frameworks. The legislative approaches towards social media, online harassment, and related issues may be scrutinized by stakeholders in Immersive technology, such as developers, international regulators, and national legislators. The objective of this assessment is to integrate safety, freedom of speech, and privacy and data security into digital platforms. The present inadequacies and deficiencies in the existing privacy regulations pertaining to the safeguarding of privacy and data protection in immersive technology highlight the ways in which we can address the difficulties associated with overseeing the storage, implementation, utilization, and commercialization of personal data within the digital environment.

As expounded in the research paper, extant measures have been implemented to safeguard users in immersive environments against potential hazards to their privacy and data security. One of the primary objectives is to examine the safeguarding of digital data against various forms of commercial exploitation on the internet. This has the potential to function as a point of reference for the development of innovative immersive interfaces that could potentially have physical or psychological ramifications. In addition, industries that are prone to instability have already initiated the incorporation of assessments based on human rights principles as outlined

by the UNDP. This measure is aimed at comprehending potential risks and offering redress in the event of any negative impacts. Taking examples from this tech firms and corporations should also taking assessments based on human rights principles.

As reiterated throughout the paper, the lack of an all-encompassing digital environment, such as the metaverse, gives rise to apprehensions pertaining to the possession of the realm. The emergence of the metaverse presents a prospect for prominent technology enterprises and corporations to establish their dominance and exert their influence over the regulation and parameters of user engagements within it. This could potentially lead to an autocratic system where users are subjected to the direct or indirect sway of these entities and their business objectives. Therefore, the governance of the metaverse presents a substantial challenge in the growth trajectory of a virtual environment such as the metaverse. Hence, it is imperative for governments, private enterprises (including prominent technology companies and corporations), global organizations, and the general public to proactively anticipate the challenges that may arise from the digital ecosystem, including concerns related to accessibility, privacy, and safeguarding of data. Thus, the author has determined that addressing concerns pertaining to immersive technologies, including access, privacy, and data protection, necessitates collaboration among various sectors, including governments, international organizations, private entities, and society. To establish a regulatory framework that is based on an informed, international, democratic consensus of the global community, rather than the commercial interests of large technology firms and corporations, is imperative.

Notwithstanding, it is imperative that these regulations account for human rights and legal concerns, including but not limited to monitoring, data collection, and the allowance of indirect advertising. Additionally, the regulations must ensure the protection of vulnerable individuals, such as children, and address contractual terms, intellectual property rights, content licensing and ownership, and the trade of digital assets. Furthermore, it is imperative for national and international regulatory bodies to acquire a comprehensive understanding of technological fundamentals and engage in collaborative efforts with major technology corporations to establish regulations. This approach is preferable to unilateral regulation or allowing technology corporations to independently govern the digital ecosystem, including the metaverse, according to their own terms and conditions. Such measures are necessary to safeguard individuals from the potential harms of surveillance capitalism perpetrated by technology corporations. In addition, it is imperative for governmental national regulators to ensure that their regulatory framework is formulated independently, devoid of any potential for

power abuse. Moreover, the regulations established by these entities must be proportionate and in tandem with the International Human Rights Law, keeping in mind the fundamental right of freedom of expression.

5.3. SUGGESTIONS

Thus, looking at the challenges such as safety, inclusivity and accessibility and the issues of privacy and data protection related to the usage of immersive technologies. The researcher suggests the following measures in order to deal with such issues and challenges:

1. To address the challenges associated with the usage of immersive technology, such as safety, inclusivity, and accessibility, by making legislation in order to address this challenge.
2. To make comprehensive international legislation for protecting Privacy and Data inside the digital ecosystem, such as the metaverse, by considering the various issues and challenges discussed in this paper.
3. To make the International and National Biometric laws congruent with the Privacy concerns and Data Protection issues related to Immersive Technologies.
4. To set up an international governing body for regulating activities undertaken under the metaverse using immersive technologies.
5. Democracies worldwide should collaborate with big tech firms to make safety measures inside the digital realm, such as the metaverse. Such a collaboration would help both parties as democracies will be able to regulate, and the big tech firms will be able to operate legally and earn profits.
6. The International governing bodies should be able also to regulate the works of the government and the tech & corporate firms and have some powers to put sanctions on the digital realm.
7. The users of such technology should have judicial and ADR systems in case there are issues inside the digital realm to find a proper remedy.

BIBLIOGRAPHY

Borak M, 'China's social app to rule them all wants to judge you for your purchases' (*South China Morning Post,* 11 January 2019) <https://www.scmp.com/abacus/tech/article/3029094/chinas-social-app-rule-them-all-wants-judge-you-your-purchases> accessed 18 May 2023.

'Registered users of Fortnite worldwide from August 2017 to May 2020' (*Statista,* 4 Jan 2023) <https://www.statista.com/statistics/746230/fortnite-players/> accessed 18 May 2023.

Kastrenakes J and Heath A, 'Facebook is spending at least $10 billion this year on its metaverse division' (*The Verge,* 26 October, 2021) <https://www.theverge.com/2021/10/25/22745381/facebook-reality-labs-10-billion-metaverse> accessed 18 May 2023.

Moynihan H, Buchser M, and Wallace J, 'What is the metaverse?' (*Chatam House,* 25 April 2022) <https://www.chathamhouse.org/2022/04/what-metaverse?gclid=Cj0KCQjwnMWkBhDLARIsAHBOftouWKQw7E-QNx2W1omWeEUcWIoCvmYjxQGsB1346RRAPmzMCjItVXgaAu-REALw_wcB> accessed 17 May 2023.

Heller B, 'Reimagining Reality: Human Rights and Immersive Technology' (2020) 008 CARR Center for Human Rights Policy Harvard Kennedy School <https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf > accessed 26 May 2023.

Dick E, 'Risks and Challenges for Inclusive and Equitable Immersive Experiences' (*Information Technology & Innovation Foundation,* 1 June 2021) <https://itif.org/publications/2021/06/01/risks-and-challenges-inclusive-and-equitable-immersive-experiences/> accessed 28 May 2023.

Ernest Cline, *Ready Player One* (Cornerstone, 2012).

Krishna Prasad S, 'Privacy and the Indian Supreme Court' National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf > accessed 1 June 2023.

Pavan Duggal, Data Protection Law in India (Universal Law Publishing, 2016).

Nelson L S., *America Identified-Biometric Technology and Society* (The MIT Press, 2010).

Citron D, *Hate Crimes in Cyberspace* (1st edn, HUP 2014).

--‘Extended Reality [XR] Market’ (*Transparency Market Research*) <https://www.transparencymarketresearch.com/extended-reality-xr-market.html> accessed 18 May 2023.

Zawadzki P et al, ‘Employee Training in an Intelligent Factory Using Virtual Reality’ (2020) IEEEAccess <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9144168> accessed 18 May 2023.

Gale S F, ‘Case study: Walmart embraces immersive learning’ (*Chief Learning Officer,* 23 March 2021) <https://www.chieflearningofficer.com/2021/03/23/case-study-walmart-embraces-immersive-learning/> accessed 18 May 2023.

Koutitas G, Smith S and Lawrence G, ‘Performance evaluation of AR/VR training technologies for EMS first responders’ (2021) Springer <https://www.researchgate.net/publication/340415977_Performance_evaluation_of_ARVR_training_technologies_for_EMS_first_responders> accessed 18 May 2023.

Makransky G, Gude S B and Mayer R, ‘Motivational and Cognitive Benefits of Training in Immersive Virtual Reality Based on Multiple Assessments’ (2019) Wiley <https://www.researchgate.net/publication/333394912_Motivational_and_Cognitive_Benefits_of_Training_in_Immersive_Virtual_Reality_Based_on_Multiple_Assessments> accessed 20 May 2023.

--‘How Virtual Reality is Transforming Education Tech and Training’ (*CBINSIGHTS,* 15 December 2020) <https://www.cbinsights.com/research/virtual-reality-education-training tech/#:~:text=The%20National%20Training%20Laboratory%20found,like%20reduced%20errors%20and%20injuries> accessed 21 May 2023.

--‘Exploring the utility of AR in Marketers’ E-Commerce Plan’ (*Snapchat,* 16 June 2022) <https://forbusiness.snapchat.com/blog/exploring-the-utility-of-ar-in-marketers-ecommerce-plan> accessed 22 May 2023.

Needham, ‘AR/VR Headset Shipments Grew Dramatically in 2021, Thanks Largely to Meta's Strong Quest 2 Volumes, with Growth Forecast to Continue, according to IDC’ (*IDC,* 21 March 2022) <https://www.idc.com/getdoc.jsp?containerId=prUS48969722> accessed 21 May 2023.

Robertson A, ‘Mark Zuckerberg has so many VR headset prototypes to show us and none of them are shipping’ (*The Verge,* 20 June 2022) <https://www.theverge.com/2022/6/20/23172503/mark-zuckerberg-meta-vr-headset-prototype-reveal-butterscotch-sunburst-holocake-mirror-lake> accessed 21 May 2023.

Balladares A, ‘Understanding Haptics for VR’ (*Virtual Reality Pop,* 3 May 2017) <https://virtualrealitypop.com/understanding-haptics-for-vr-2844ed2a1b2f> accessed 21 May 2023.

--‘Haptic Technology Market (By Component: Solution, Software; By Application: Consumer Electronics, Gaming, Healthcare, Robotics, Education, Research, Others; By Feedback Type: Tactile, Force) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2022-2030’ (*Precedence Research,* September 2022) <https://www.precedenceresearch.com/haptic-technology-market> accessed 21 May 2023.

Dzyuba A, ‘Immersive Experience: The Definition, The Technology and the Future’ (*Forbes,* 2 Jan 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/01/02/immersive-experience-the-definition-the-technology-and-the-future/?sh=304efd5f4e0d> accessed 23 May 2023.

Bhanji Z, ‘A New Reality: How VR Actually Works’ (*MEDIUM,* 2 Oct 2018) <https://medium.com/predict/a-new-reality-how-vr-actually-works663210bdff72> accessed 23 May 2023.

--‘Field of View for Virtual Reality Headsets Explained’ (*VR LENS LAB*) <https://vr-lens-lab.com/field-of-view-for-virtual-reality-headsets/> accessed 23 May 2023.

Horwitz J, ‘HTC Vive Pro Eye hands-on: Gaze into VR’s future with foveated rendering’ (*VENTUREBEAT,* 10 January 2019) <https://venturebeat.com/business/htc-vive-pro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 23 May 2023.

Strickland J, ‘How Virtual Reality Works’ (*Howstuffworks)* <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed 23 May 2023.

--‘A Quick Guide to Degrees of Freedom in Virtual Reality’ (*Kei Studios,* 2018), <https://kei-studios.com/quick-guide-degrees-of-freedomvirtual-reality-vr/> accessed on 24 May 2023.

--‘Understanding Sensors: Magnetometers, Accelerometers and Gyroscopes’ (*Virtual Reality Society,* 2017) <https://www.vrs.org.uk/virtual-reality-gear/motion-tracking/sensors.html> accessed on 23 May 2023.

--Meta Quest Blog, ‘Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR’ (*Meta,* 25 Sep 2019) <https://www.meta.com/blog/quest/introducing-hand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed on 24 May 2023.

--‘Latency - Virtual Reality and Augmented Reality’ (*VR AR & XR WIKI*) <https://xinreality.com/wiki/Latency> accessed on 24 May 2023.

Strickland J, ‘How Virtual Reality Works’ (*Howstuffworks*) <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed 24 May 2023.

Horwitz J, ‘HTC Vive Pro Eye hands-on: Gaze into VR’s future with foveated rendering’ (*Venturebeat,* 10 January 2019) <https://venturebeat.com/business/htc-vive-pro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 25 May 2023.

Johnson P, ‘Spatial Computing: An Overview for out Techie Friends’ (*Magic Leap,* 27 August 2018) <https://www.magicleap.com/blog-staging/spatial-computing-an-overview-for-our-techie friends#: ~:text=Spatial%20computing%20is%20about%20volumes, access%20through%20Magic%20Leap%20One.> accessed 25 May 2023.

Strickland J, ‘How Virtual Reality Works’ (*Howstuffworks*) <https://electronics.howstuffworks.com/gadgets/other-gadgets/virtual-reality.htm> accessed on 25 May 2023.

Suovanen J et al, ‘Magic Leap One Teardown’ (*IFIXIT,* 23 August 2018) <https://bit.ly/2Z2Df4L> accessed 25 May 2023.

Vigliarolo B, ‘Microsoft HoloLens: Cheat Sheet’ (*TECHREPUBLIC,* 30 July 2018) <https://tek.io/3bqSC9G> accessed 25 May 2023; Ash, ‘Sorry Microsoft, Controllers Are a Must for AR Smart Glasses’ (*Medium,* 13 September 2019) <https://bit.ly/2LrS5K1c> accessed 25 May 2023.

Webster A, ‘Fortnite’s Marshmello concert was the game’s biggest event ever’ (*The Verge,* 21 February 2019) <https://www.theverge.com/2019/2/21/18234980/fortnite-marshmelloconcert-viewer-numbers> accessed 25 May 2023.Rack S, ‘How Pokémon Go has changed my life’ (*BBC News,* 1 January 2020) <https://bbc.in/2WX6C5S> accessed 25 May 2023.

Hoium T, ‘Oculus Devices Sold Out in a Positive Sign for Virtual Reality’ (*The Motley Fool,* 27 December 2019) <https://www.fool.com/investing/2019/12/27/oculus-devices-sold-out-in-positive-sign-for-virtu.aspx> accessed 26 May 2023.

Agrawal A.J., ‘3 reasons augmented reality has not achieved widespread adoption’ (*The Next Web,* 16 February 2018) <https://thenextweb.com/contributors/2018/02/16/3-reasons-augmented-reality-hasnt-achieved-widespread-adoption/> accessed 26 May 2023.

‘Hate in Social VR’ (*Anti-Defamation League,* 7 December 2018) https://www.adl.org/resources/reports/hate-in-social-virtual-reality accessed 26 May 2023

‘The Blu Franchise’ (*Wevr*) <https://wevr.com/theblu> accessed 26 May 2023.

‘Best VR Underwater Adventure Games for Deep-Sea Explorers’ (*VRGAMECRITIC*) <https://vrgamecritic.com/article/best-vr-underwater-exploration-adventure-games> accessed 26 May 2023.

Cummings J.N. & Bailenson J.J., ‘How immersive is enough? A meta-analysis of the effect of immersive technology on user presence’ (2016) VHIL <https://vhil.stanford.edu/pubs/2016/how-immersive-is-enough/> accessed 26 May 2023.

Johnson E, ‘Full transcript: Stanford virtual reality expert Jeremy Bailenson on Too Embarrassed to Ask’ (*VOX,* 4 August 2016) < https://www.vox.com/2016/8/4/12371450/jeremy-bailenson-stanford-university-virtual-reality-too-embarrassed-to-ask-podcast-transcript> accessed 26 May 2023.

Bailenson J, *Experience on Demand: What Virtual Reality Is, How It Works, And What It Can Do* (1st edn, W.W. Norton & Company 2018) 17-20.

Cortese, Michelle and Zeller A, ‘Designing Safer Social VR’ (*Medium,* 2 November, 2019) <https://immerse.news/designing-safer-social-vr-76f99f0be82e> accessed 26 May 2023.

--‘Virtual reality eases phantom limb pain’ (*Sciencedaily,* 31 May 2017) <https://www.sciencedaily.com/releases/2017/05/170531102921.htm.> accessed 26 May 2023.

Duggan M, ‘Online Harassment 2017’ (Pew Research Center, 11 July 2017) <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/> accessed 26 May 2023.

Brown T.I.et. al*,* ‘Prospective Representation of Navigational Goals in the Human Hippocampus’ (2016) 352 Science 1323.

Understanding Sensors: Magnetometers, Accelerometers and Gyroscopes’ (*Virtual Reality Society,* 2017), <https://www.vrs.org.uk/virtual-reality-gear/motion-tracking/sensors.html> accessed 26 May 2023.

‘Ubiquitous $90 billion AR to dominate focused $15 billion VR by 2022’ (*Techcrunch,* 26 January 2018) <https://techcrunch.com/2018/01/25/ubiquitous-ar-to-dominate-focused-vr-by-2022/> accessed 26 May 2023.

Robertson A, ‘Tesla suit’s new VR gloves let you feel virtual objects and track your pulse’ (*The Verge,* 27 December 2019) <https://bit.ly/2T2XcEv> accessed 26 May 2023.

Citron D, ‘Cyber Civil Rights’ (2009) 89 Boston Univ. Law Rev.66 <https://ssrn.com/abstract=1271900> accessed 26 May 2023.

Prince M, 'WHY WE TERMINATED DAILY STORMER' (*Cloudflare,* 17 August 2017) <https://blog.cloudflare.com/why-we-terminated-daily-stormer/> accessed 26 May 2023.

Frystyk H, 'The Internet Protocol Stack' (*w3 org,* July 1994) <https://www.w3.org/People/Frystyk/thesis/TcpIp.html> accessed 26 May 2023.

Lorenz T, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here is Why I Keep Going Back' (*Mic,* 26 May 2016) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> 27 May 2023.

Belamire J, 'My First Virtual Reality Groping' (*Medium,* 20 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 27 May 2023.

Outlaw J, 'Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users' (*Medium,* 4 April 2018) <https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers> accessed 27 May 2023.

Cortese M and Zeller A, Designing Safer Social VR, (*Medium,* 2 November 2019) <https://immerse.news/designing-safer-social-vr76f99f0be82e> accessed 27 May 2023.

Tabahriti S, 'Meta is putting a stop to virtual groping in its metaverse by creating 4-foot safety bubbles around avatars' (*Business Insider India,* 5 February 2022) <https://www.businessinsider.in/tech/news/meta-is-putting-a-stop-to-virtual-groping-in-its-metaverse-by-creating-4-foot-safety-bubbles-around-avatars/articleshow/89367619.cms> accessed 27 May 2023.

Sullivan M, 'Virtually violated: How Facebook is trying to fix abuse on social VR before it goes mainstream' (*Fast Company,* 5 February 2019) <https://www.fastcompany.com/90342844/abuseon-social-vr-facebook-is-trying-to-fix-it-before-it-goes-mainstream> accessed 27 May 2023.

Lemley M and Volokh E, 'Law, Virtual Reality, and Augmented Reality' (2018) 166 U. PA. L. REV., 87-88.

--Meta Quest Blog, 'Introducing 'Facebook Horizon,' a New Social VR World, Coming to Oculus Quest and the Rift Platform in 2020' (*Meta,* 25 September 2019) < https://www.meta.com/blog/quest/introducing-facebook-horizon-a-new-social-vr-world-coming-to-oculus-quest-and-the-rift-platform-in-2020/> accessed 28 May 2023.

--Meta Quest Blog, 'Introducing New Features from Facebook to Help People Connect in VR and an Update to Our Privacy Policy' (*Meta,* 11 December 2019) <

https://www.meta.com/blog/quest/introducing-new-features-from-facebook-to-help-people-connect-in-vr-and-an-update-to-our-privacy-policy/> accessed 28 May 2023.

Petrock V, 'US Virtual and Augmented Reality Users 2021' (*Insider Intelligence,* 15 April 2021) <https://wwwemarketer.com/content/us-virtual-augmented-reality-users-2021> accessed 28 May 2023.

Dick E, 'Balancing Privacy and Innovation in Augmented and Virtual Reality' (*Information Technology and Innovation Foundation,* March 4, 2021) <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> accessed 28 May 2023.

Franks M A, 'The Desert of the Unreal: Inequality in Virtual and Augmented Reality' (2017) 51 UC Davis Law Review <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Franks.pdf> accessed 28 May 2023.

Dick E, 'How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces' (*Information Technology and Innovation Foundation,* 14 December 2021) <https://itif.org/person/ellysse-dick.> accessed 28 May 2023.

Bertrand P et al, 'Learning Empathy through Virtual Reality: Multiple Strategies for Training Empathy-Related Abilities Using Body Ownership Illusions in Embodied Virtual Reality' (*Front Robot AI,* 2018) <https://www.frontiersin.org/articles/10.3389/frobt.2018.00026/full> accessed 28 May 2023.

Outlaw J and Duckles B, 'Why Women Don't Like Virtual Reality: A Study of Safety, Useability, and Self-Expression in Social VR' (*The Extended Mind,* 16 October 2017) <https://static1.squarespace.com/static/60e8ceb4ae52881d57698bf6/t/6164b95156a52d3614c29e82/1633990999726/The-Extended-Mind_Why-Women-Don%27t-Like-Social-VR_2017.pdf> accessed 29 May 2023.

Robertson A, 'TikTok Prevented Disabled Users' Videos from Showing Up in Feeds' (*The Verge,* 2 December 2019) <https://www.theverge.com/2019/12/2/20991843/tiktok-bytedance-platform-disabled-autism-lgbt-fat-user-algorithm-reach-limit.> accessed 29 May 2023.

Stanney K et al., 'Virtual Reality is Sexist: But It Does Not Have to Be' (*Frontiers in Robotics and AI,* 31 January 2020) < https://www.frontiersin.org/articles/10.3389/frobt.2020.00004/full> accessed 29 May 2023.

Mboya A M, 'The Oculus Go Wasn't Designed for Black Hair' (*Debugger,* 5 November 2020) <https://debugger.medium.com/the-oculus-go-a-hard-ware-problem-for-black-women-225d9b48d098.> accessed 29 May 2023.

--'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (*XR Association,* October 2020) <https://xra.org/wp-content/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 29 May 2023.

Phillips K U, 'Virtual Reality Has an Accessibility Problem' (*Scientific American,* January 29 2020) <https://blogs.scientificamerican.com/voices/virtual-reality-has-an-accessibility-problem> accessed 29 May 2023.

--'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (*XR Association,* October 2020) <https://xra.org/wpcontent/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 29 May 2023.

Wong A et al, 'VR Accessibility Survey for People with Disabilities' (*Disability Visibility Project*) <https://www.ben-peck.com/papers/VR_Accessibility_Survey.pdf> accessed 29 May 2023.

Connor J O et. al, 'XR Accessibility User Requirements' (*W3C Working Draft,* 16 September 2020) <https://wwww3.org/TR/xaur> accessed 29 May 2023.

Cheng R, 'Can 5G Make Smart Glasses Cool?' (*Cnet,* 1 March 2018) <https://www.cnet.com/news/can-5g-make-smart-glasses-cool-ericsson-odg-mwc-2018.> accessed 29 May 2023.

Anderson M, 'About a Quarter of Rural Americans Say Access to High-Speed Internet is a Major Problem' (*Pew Research Center,* 10 September 2018) <https://www.pewresearch.org/fact-tank/2018/09/10/about-a-quarter-of-rural-americans-say-access-to-high-speed-internet-is-a-major-problem.> accessed 29 May 2023.

Brake D and Bruer A, 'How to Bridge the Rural Broadband Gap Once and for All' (*Information Technology and Innovation Foundation,* 22 March 2021) <https://itif.org/publications/2021/03/22/how-bridge-rural-broadband-gap-once-and-all/> accessed 29 May 2023.

Brewster S, 'The Best VR Headset: But What About Mobile VR?' (*The New York Times,* 3 November 2020) <https://www.nytimes.com/wirecutter/reviews/best-standalone-vr-headset/#what-about-mobile-vr.> accessed 29 May 2023.

Valishery L S, 'Reported Price of Leading Consumer Virtual Reality (VR) Headsets in 2019, by Device' (*statista,* 22 January 2021)

<https://www.statista.com/statistics/1096886/reported-price-of-leading-consumer-vr-headsets-by-device.> accessed 30 May 2023.

Subin S, 'Is 2021 Finally the Year for Smart Glasses? Here's Why Some Experts Still Say No' (*CNBC,* 23 January 2021) <https://www.cnbc.com/2021/01/23/why-experts-dont-expect-smart-glasses-to-surge-in-2021.html.> accessed 30 May 2023.

Anderson M and Perrin A, 'Tech Adoption Climbs Among Older Adults: Barriers to Adoption and Attitudes Towards Technology' (*Pew Research Center,* May 17, 2017) <https://www.pewresearch.org/internet/2017/05/17/barriers-to-adoption-and-attitudes-towards-technology.> accessed 30 May 2023.

Horrigan J B, 'Digital Readiness Gaps' (*Pew Research Center,* 20 September 2016) <https://www.pewresearch.org/internet/2016/09/20/digital-readiness-gaps.> accessed 30 May 2023.

Anderson M and Perrin A, 'Disabled Americans are Less Likely to Use Technology' (*Pew Research Center,* 7 April 2017) <https://www.pewresearch.org/fact-tank/2017/04/07/disabled-americans-are-less-likely-to-use-technology.> accessed 30 May 2023.

Bye K and Outlaw J, 'Elements of Culture and Cultivating Community with Jessica Outlaw' (*Voices of VR Podcast,* 6 July 2019) <http://voicesofvr.com/784-elements-of-culture-cultivating-community-with-jessica-outlaw.> accessed 31 May 2023.

McGee E, 'Black Genius, Asian Fail: The Detriment of Stereotype Lift and Stereotype Threat in High-Achieving Asian and Black STEM Students' (*AERA Open,* 5 December 2018), <https://doi.org/10.1177%2F2332858418816658.> accessed 31 May 2023.

Brown L X.Z. et. al, 'Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?' (*Center for Democracy and Technology,* 3 December 2020) <https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination.> accessed 31May 2023.

-- 'XRA'S DEVELOPERS GUIDE, CHAPTER THREE: Accessibility & Inclusive Design in Immersive Experiences' (XR Association, October 2020) <https://xra.org/wpcontent/uploads/2020/10/xra_dev_guide_chapter3.pdf> accessed 31 May 2023.

McGinley M K. et. al, 'The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States' (2023) XIII THE NATIONAL LAW REVIEW <https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states> accessed 31 May 2023.

--Meta Quest Blog, 'Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR' (*Meta,* 25 September 2019) <https://www.oculus.com/blog/introducinghand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed 31 May 2023.

--'#517: Biometric Data Streams & the Unknown Ethical Threshold of Predicting & Controlling Behaviour' (*Voices of VR Podcast,* 20 March 2017) <http:// voicesofvr.com/517-biometric-data-streams-the-unknown-ethical-threshold-of-predicting-controlling-behavior/> accessed 31 May 2023.

Sirois S & Brisson J, 'Pupillometry' (2014) 5 Wires Cognitive Science <https://onlinelibrary.wiley.com/doi/abs/10.1002/wcs.1323> 679–692.

Farnsworth B, 'Pupillometry 101: What You Need to Know' (*IMOTIONS*) <https://imotions.com/blog/pupillometry-101/> accessed 1 June 2023.

Bar-Zeev A, 'The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail' (*VICE,* 28 May 2019) < https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail> accessed 1 June 2023.

--'How Does Eye Tracking Work?' (*VR.org,* 22 February 2018) <https://www.vr.org/2018/02/22/how-does-eye-tracking-work/> accessed 1 June 2023.

Klaris E & Bedat A, 'VR & AR: Virtual Reality, Augmented Reality & Biometric Data after 2017-Ed Klaris & Alexia Bedat' (*MEDIUM,* 1 February 2018) <https://blog.klarislaw.com/vr-ar-virtual-reality-augmented-reality-biometric-data-after-2017-ed-klaris-alexia-bedat-a15e9cb000a1> accessed 1 June 2023.

--Tobii Homepage, (*Tobii*) < https://developer.tobii.com/xr/> accessed 1 June 2023.

Horwitz J, 'HTC Vive Pro Eye hands-on: Gaze into VR's future with foveated rendering' (*Venturebeat,* 10 January 2019) <https://venturebeat.com/2019/01/10/htc-vivepro-eye-hands-on-gaze-into-vrs-future-with-foveated-rendering/> accessed 1 June 2023.

'What is Privacy' (Privacy International, 23 October 2017) <https://privacyinternational.org/explainer/56/what-privacy> accessed 1 June 2023.

Krishna Prasad S et al, 'Privacy and the Indian Supreme Court' National Law University Delhi Press <https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/Privacy_and_the_Indian_Supreme_Court_1.pdf > accessed 1 June 2023.

--'Cisco predicts 15b connected devices by 2015' (*edge,* 14 June 2011) <https://www.itp.net/news/585110-cisco-predicts-15b-connected-devices-by-2015> accessed 2 June 2023.

--‘The XRSI Privacy Framework version 1.0’ (*XRSI,* September 2020) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 2 June 2023.

Castro D and McQuinn A, ‘ITIF Filing to FTC on Informational Injury Workshop’ (*Information Technology and Innovation Foundation,* October 27, 2017) <http://www2itif.org/2017-informational-injury-comments.pdf> accessed 2 June 2023.

O’Brolcháin F et al, ‘The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy’ (2016) Science and Engineering Ethics 22 <https://doiorg/10.1007/s11948-014-9621-1> accessed 2 June 2023.

Patel N, ‘Handset Data Traffic’ (Strategy Analytics, 18 June 2012) <https://www.strategyanalytics.com/access-services/media-and-services/mobile/wireless-media/wireless-media/reports/report-detail/handset-data-traffic-(2001-2017)> accessed 2 June 2023.

--‘India Internet Usage Stats and Telecommunications Market Report’ (Inter World Stats, 2016) <https://www.internetworldstats.com/asia/in.htm> accessed 2 June 2023.

--Cyber Civil Rights Initiative, ‘46 States + DC + One Territory Now Have Revenge Porn Laws’ <https://wwwcybercivilrights.org/revenge-porn-laws> accessed 2 June 2023.

--Kei Studios, ‘A Quick Guide to Degrees of Freedom in Virtual Reality’ <https://kei-studioscom/quick-guide-degrees-of-freedom-virtual-reality-vr> accessed 3 June 2023.

--Meta Quest Blog, ‘Introducing Hand Tracking on Oculus Quest—Bringing Your Real Hands into VR,” (*Meta,* 25 September 2019) <https://www.meta.com/blog/quest/introducing-hand-tracking-on-oculus-quest-bringing-your-real-hands-into-vr/> accessed 3 June 2023.

--HTC, ‘HTC’s VIVE Eye Tracking data collection: HTC Terms: Learn More’ <https://wwwhtc.com/us/terms/learn-more> accessed 20 June 2023.

--VIVE Enterprise, ‘VIVE Pro Eye Office’ https://enterprisevive.com/us/product/vive-pro-eye-office accessed 4 June 2023.

Hayden S, ‘Valve Psychologist: Brain-Computer Interfaces Are Coming & Could Be Built into VR Headsets’ (*Road to VR,* 23 March 2019) <https://wwwroadtovr.com/valve-brain-computer-interfaces-vr-ar-gdc-2019> accessed 4 June 2023.

Ghose T, ‘Eye Tracking Could Diagnose Brain Disorders’ (*Live Science,* 18 September 2012) <https://wwwlivescience.com/23274-eye-tracking-gaze-brain-disorders.html> accessed 4 June 2023.

Liu A, 'Why VR Analytics is Critical to Prove ROI' (*cognitive3D blog,* 3 December 2019) <https://contentcognitive3d.com/vr-merchandising-case-study> accessed 4 June 2023.

--The XR Safety Initiative, '156: Child Safety' (*XRSI Privacy Framework Version 1.0.,* September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 4 June 2023.

Christensen D and Jimenez D, 'Data Protection Should Extend to Virtual Places and Data Objects' (*IAPP Privacy Perspectives, 24 August 2016*) <https://iapporg/news/a/data-protection-should-extend-to-virtual-places-and-data-objects> accessed 4 June 2023.

--US Equal Employment Opportunity Commission, 'Laws Enforced by EEOC' (*eeoc.gov,* 10 February 2021) <https://wwweeoc.gov/statutes/laws-enforced-eeoc> accessed 4 June 2023.

--US Department of Justice Civil Rights Division, 'The Fair Housing Act' (*justice.gov,* 10 February 2021) <https://wwwjustice.gov/crt/fair-housing-act-1> accessed 4 June 2023.

--US. Department of Labor Employee Benefits Security Administration, 'FAQs on HIPAA Portability and Non-discrimination Requirements for Employers and Advisers' (*U.S. Department of Labor*) <https://wwwdol.gov/sites/dolgov/files/ebsa/about-ebsa/our-activities/resource-center/faqs/hipaa-compliance.pdf> accessed 4 June 2023.

Matsakis L, 'The Supreme Court Just Greatly Strengthened Digital Privacy' (*Wired,* 22 June 2018) <https://wwwwired.com/story/carpenter-v-united-states-supreme-court-digital-privacy> accessed 4 June 2023.

Han S et al, 'Using Deep Neural Networks for Accurate Hand-Tracking on Oculus Quest' (*Facebook AI,* 25 September 2019) <https://aifacebook.com/blog/hand-tracking-deep-neural-networks> accessed 4 June 2023.

Stein S, 'Mind Control Comes to VR, Letting Me Explode Alien Heads with a Thought' (*cnet,* January 30, 2021) <https://wwwcnet.com/news/controlling-vr-with-my-mind-nextminds-dev-kit-shows-me-a-strange-new-world> accessed 5 June 2023.

Kroger J L et al, 'What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking' (2020) IFIP Advances in Information and Communication Technology 576 <https://doiorg/10.1007/978-3-030-42504-3_15> accessed 5 June 2023.

Acosta N, 'Are IP Addresses 'Personal Information' Under CCPA?' (*IAPP Privacy Advisor,* 28 April 2020) <https://iapporg/news/a/are-ip-addresses-personal-information-under-ccpa> accessed 5 June 2023.

--XR Safety Initiative, '341.1: FERPA: Protection of Education Record Considerations' (*The XRSI Privacy Framework Version 1.0.,* September 2019) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 5 June 2023.

O'Brolchain F et al, 'The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy' (2015) Springer Link <https://link.springer.com/article/10.1007/s11948-014-9621-1> accessed 5 June 2023.

Bailenson J, 'Protecting Nonverbal Data Tracked in Virtual Reality' (*JAMA Paediatrics,* August 6 2018) <https://vhilstanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf> accessed 11 June 2023.

Jerome J, 'Establishing Privacy Controls for Virtual Reality and Immersive Technology,' (IAPP Privacy Perspectives, *September 9, 2020*) <https://iapporg/news/a/establishing-privacy-controls-for-virtual-reality-and-immersive-technology> accessed 11 June 2023.

Miller M R et al, 'Personal Identifiability of User Data During Observation of 360-Degree VR Video' (2020) 10 Scientific Reports <https://doiorg/10.1038/s41598-020-74486-y> accessed 12 June 2023.

Egan E, 'IIC: New Technologies and Interfaces in Communicating About Privacy: Towards People-Centered and Accountable Design' (*Facebook,* July 2020) <https://aboutfb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf> accessed 12 June 2023.

Outlaw J and Persky S, 'Industry Review Boards are Needed to Protect VR User Privacy' (*World Economic Forum,* August 29, 2019) <https://wwwweforum.org/agenda/2019/08/the-hidden-risk-of-virtual-reality-and-what-to-do-about-it> accessed 12 June 2023.

Cavoukian A and Castro D, 'Big Data and Innovation, Setting the Record Straight: De-Identification Does Work' (*Information Technology and Innovation Foundation,* 16 June 2014) <https://www2.itif.org/2014-big-data-deidentification.pdf> accessed 12 June 2023.

--New York State Senate, 2017-2018 legislative session, A8155B <https://wwwnysenate.gov/legislation/bills/2017/a8155> accessed 15 June 2023.

--US Federal Trade Commission, 'Complying with COPPA: Frequently Asked Questions' (*ftc.gov,* accessed 10 February 2021) <https://wwwftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 15 May 2023.

--US Department of Justice Office of Privacy and Civil Liberties, 'Overview of the Privacy Act of 1974 (2020 Edition)' (*justice.gov,* 10 February 2021)

<https://wwwjustice.gov/opcl/overview-privacy-act-1974-2020-edition> accessed 16 May 2023.

Matsakis L, 'The Supreme Court Just Greatly Strengthened Digital Privacy' (*WIRED,* 22 June 2018) <https://wwwwired.com/story/carpenter-v-united-states-supreme-court-digital-privacy> accessed 16 May 2023.

Emmerman R D et al, 'New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies' (*Loeb & Loeb,* March 2018) <https://wwwloeb.com/en/insights/publications/2018/03/new-biometric-information-privacy-cases-reveal-b> accessed 16 May 2023.

Christensen D and Jimenez D, 'Data Protection Should Extend to Virtual Places and Data Objects' (*IAPP Privacy Perspectives,* 24 August 2016) <https://iapporg/news/a/data-protection-should-extend-to-virtual-places-and-data-objects> accessed 18 June 2023.

--US Federal Trade Commission, 'FTC Provides Additional Guidance on COPPA and Voice Recordings' (*ftc.gov,* 23 October 2017) <https://wwwftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings> accessed 18 June 2023.

McQuinn A and Castro D, 'A Grand Bargain on Data Privacy Legislation for America' (*Information Technology and Innovation Foundation,* 14 January 2019) <https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america/> accessed 18 June 2023.

--'XRSI Privacy Framework Version 10' (*XRSI,* September 2020) <https://xrsi.org/wp-content/uploads/2020/09/XRSI-Privacy-Framework-v1_002.pdf> accessed 19 June 2023

Vinje J E, 'Privacy Manifesto for AR Cloud Solutions' (*Open AR Cloud on Medium,* 17 October 2018) <https://mediumcom/openarcloud/privacy-manifesto-for-ar-cloud-solutions-9507543f50b6> accessed 19 June 2023

--XR Association, 'Research & Best Practices' (*xraorg,* 10 Febraury 2021) <https://xraorg/research-best-practices> accessed 19 June 2023.

--National Institute of Standards and Technology, 'NIST Privacy Framework' (*US Department of Commerce National Institute of Standards and Technology,* 16 January 2020) <https://wwwnist.gov/system/files/documents/2020/01/16/NIST Privacy Framework_V1.0.pdf> accessed 19 June 2023.

--Meta Quest, 'Oculus Connect 6: Introducing Hand Tracking on Oculus Quest, Facebook Horizon and More' (*Meta,* 25 September 2023)

<https://about.fb.com/news/2019/09/introducing-hand-tracking-on-oculus-quest-facebook-horizon-and-more/> accessed 20 June 2023.

--'Using deep neural networks for accurate hand-tracking on Oculus Quest' (*Meta,* 25 September 2019) <https://bit.ly/2ZoQVHw> accessed 20 June 2023.

--'NextMind Unveils World's First Brain-Sensing Wearable That Delivers Real-Time Device Control with Just Your Thoughts' (*Businesswire,* 21 November 2019) <https://www.businesswire.com/news/home/20191121005757/en/NextMind-Unveils-Worlds-First-Brain-Sensing-Wearable-That-Delivers-Real-Time-Device-Control-With-Just-Your-Thoughts> accessed 20 June 2023.

Hsu J, 'Real "Westworld" Haptic Vests Better Than Fiction' (*Discover Magazine,* 8 June 2018) <https://www.discovermagazine.com/technology/real-westworld-haptic-vests-better-than-fiction> accessed 24 June 2023

--TRIPP: Fitness for your Inner Self, TRIPP, <https://www.tripp.com/> accessed 24 June 2023.

Chin J, 'Chinese Police Add Facial-Recognition Glasses to Surveillance Arsenal' (*The Wall Street Journal,* 7 February 2018) <https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353.> accessed 24 June 2023.

Restar A1, 'US Army Is Testing Facial Recognition Goggles' (*Z6 MAG,* 22 July 2019) <https://z6mag.com/2019/07/22/us-army-is-testing-facial-recognition-goggles/> accessed 24 June 2023.

Ghose T, 'Eye Tracking Could Diagnose Brain Disorders' (*Live Science,* 18 September 2012) <https://www.livescience.com/23274-eye-tracking-gazebrain-disorders.html> accessed 24 June 2023.

Schultz D, 'Alzheimer's disease tied to brain's navigation network' (*Science,* 22 October 2015) <https://www.sciencemag.org/news/2015/10/alzheimers-disease-tied-brain-s-navigation-network> accessed 24 June 2023.

Lemley M & Volokh E, 'Law, Virtual Reality, and Augmented Reality' (2018) 166 University of Pennsylvania Law Review 28-29.

Cortese M & Zeller A, 'How to protect users from harassment in social VR spaces' (*The Next Web,* 2 January 2020) <https://thenextweb.com/syndication/2020/01/02/how-to-protect-users-from-harassment-in-social-vr-spaces/> accessed 25 June 2023.

Lorenz T, 'Virtual Reality Is Full of Assholes Who Sexually Harass Me. Here is Why I Keep Going Back' (*Mic, 26 May 2016*) <https://www.mic.com/articles/144470/sexual-harassment-in-virtual-reality> accessed 26 June 2023.

Matias J. N, ‘Posting Rules in Online Science Discussions Prevents Problems & Increases Participation’ (*Civilservant,* April 2019) <http://civilservant.io/r_science_sticky_coments_1.html> accessed 26 June 2023.

UN Human Rights Council, Protect, respect and remedy : a framework for business and human rights : report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, 7 April 2008, A/HRC/8/5, <https://www.refworld.org/docid/484d2d5f2.html> accessed 30 June 2023.