Usable Privacy for Biometric Data in XR

Sonal Lakhotia
Institute of Computer Science
University of Göttingen
Göttingen, Germany
Email: sonal.lakhotia@stud.uni-goettingen.de

***Abstract*—XR technologies find usage in a plethora of domains. Availability and reduced hardware costs enable widespread adoption of XR in almost every sector. User data such as demographic and biological details, location, movement, and biometrics empower XR devices to create a virtual environment. The collected user data might contain sensitive, identifying, or personal information. AR/VR devices can combine all collected information and deduce additional details about an individual user. Biometric data collected in mundane experiments in which subjects perform repetitive tasks could be used to uniquely identify an individual and is subject to ethical and legal debate[1]. If misused, inferred biometric data and behavioral biometrics endanger the autonomy and anonymity of the user. Privacy concerns about using biometric data and privacy risk mitigation approaches are crucial in XR development. The report discusses the usability of biometric data and privacy concerns.**

***Index Terms*—Biometric data, Privacy, XR, Behavioural Biometrics**

I. Introduction

XR (Extended Reality) suite composes virtual, augmented, and mixed reality technologies. A virtual reality experience is more immersive as compared to augmented and mixed reality as the VR device completely blocks the user's vision and other senses while an AR device overlays the digital elements in the user's realization of physical space and a mixed reality device controls the user's field of view. [2].

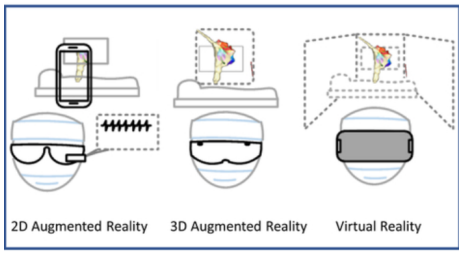

Fig. 1. Extended Reality Suite [3]

Figure 1 depicts the convergence of physical and digital realities in XR. 2D Augmented Reality (AR) devices can be worn on the head or displayed on a phone or tablet screen using a camera to represent physical reality. 3D Augmented Reality devices use spatial mapping techniques to show 3D objects in the physical environment, and virtual reality (VR) devices block the user's view with a virtual environment.[3]. XR finds extensive use in domains like Retail, construction, media, healthcare, education, gaming and entertainment, automotive, aerospace, and defense[4]. Application areas of these technologies include training and simulation, research and development, maintenance, medical, and therapy. XR devices and associated adjuncts enable a vast range of data collection:

1) Physical actions and movements that include optical and inertial tracking of head/body/limb movements [5], recognizing facial expressions, EMG neuromotor input, and speech recognition.
2) Neural Activity such as EEG for brain-computer interfaces [5].
3) Context includes location tracking, optical data analysis using machine learning, and SLAM (Simultaneous Localization and Mapping)[5].
4) Physiology encompasses gaze tracking, eye tracking, HRV sensing, and other biometrics such as heart rate, respiration, pulse oximetry, and blood pressure[5].

Physical and Virtual worlds are becoming convergent with XR. A VR social network - Horizon, launched by Facebook in 2020, is capable of VR penetration even deeper if Facebook users join the platform [4]. Horizon is a part of a much broader spectrum called Metaverse. It is defined as internet-connected virtual, augmented, and mixed reality worlds [4]. Metaverse offers semi or fully immersive experiences to users. Users can represent themselves as avatars and interact with other avatars in multiple physical and virtual spaces. Human interaction and artificially intelligent entities control the avatars in a virtual environment [4]. When a user interacts with the virtual environment, a continuous data stream is generated, which enables the sensors and displays in AR/VR devices to create an immersive sense of occlusion. Avatars of self and other users impact the task efficiency compared to no avatars depicting any user in the virtual environment. It creates a cooperative and competitive environment for task completion as in the real world [6].

Virtual reality social networks impose privacy threats, the primary concerns being the misuse and vulnerability of data. The unintentional revelation of user information and problems related to associational privacy and loss of anonymity leads to users' privacy breaches. Threats could be associated with data manipulation and cause people to feel that they are living under surveillance [7]. Privacy risks are associated when dealing with sensitive information about users' biometrics. Biometrics is an old idea and method of recognizing people. The face was

to distinguish between the known and the unknown. It is an ancient and rudimentary example of biometrics since the earliest days of civilization, [8]. Biometric data characterize users' personal information, such as specific physical, behavioral or physiological attributes. Figure 2 describes the physiological and behavioral biometrics capable of user identification and authentication. Biometric data accounts for unique information from a user's face, fingerprint, voice, or DNA. It is crucial to mitigate privacy risks associated with biometric data collected by an AR/VR device that can be transferred to third parties or used by the manufacturing company for product improvement.

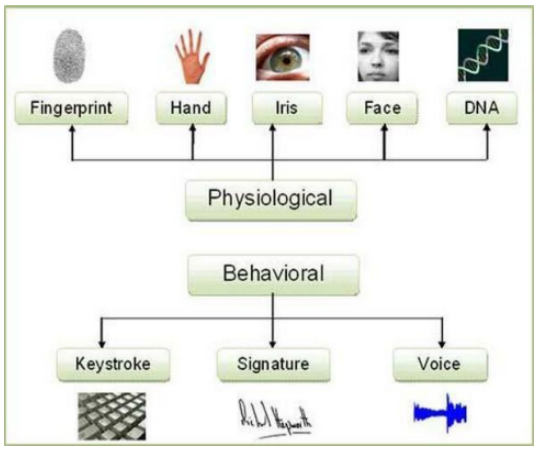

Fig. 2. Classification of biometrics [8]

Biometrics are advantageous for maintaining security and authentication in devices as it provides an improved customer experience and safety. The authentication data is not lost or forgotten, reducing maintenance and operational costs. A few shortcomings are also associated with device authentication using biometrics. It might require additional hardware integration. Measurements could be affected by hardware or the user's physical space. There is a possibility that biometric authentication would not suffice for device security as the device does not measure biometrics accurately.

II. Usability of Biometric data in XR

Reconstructing physical sensations in a virtual environment delivers a fully immersive virtual reality experience for the user. User body movements are tracked to collect biometric data so that users' actions in physical space can be replicated in virtual space. Biometric tracking is not limited to body movement and coordination in immersive environments. It includes a collection of personal data such as full body tracking, eye tracking, hand movements, and head orientation. Biometric data complements XR technology by extensive monitoring and feedback of the user's blood pressure, heart rate, respiration rate, and pulse oximetry. The collection of sensitive data enables the creation of an even more immersive experience for the user.

Internal cameras in VR devices are used for eye tracking. It collects data concerning the user's field of vision, the object at which the user is looking, changes in pupil size due to different virtual entities in the virtual environment, and the opening and closing of the user's eyes. An avatar reflecting all these eye movements and expressions in a virtual environment makes the VR experience even more immersive.

Gaze tracking capabilities allow VR displays to use foveal rendering, which simulates the human field of vision by reducing the resolution of screens that appears in a user's actual peripheral vision [4]. It makes the virtual experience more realistic and reduces the strain on the eyes of the users. It allows users to display better quality pictures at the focal point and reduces latency which is considered a contributor to motion sickness in immersive experiences[4].

Brain-Computer Interface (BCI) technologies are far more advanced than eye tracking. It measures brain activity and adapts and responds to neural signals from the user. Specific needs of the user in the virtual environment can be met using these signals. Example: Wearable devices such as AR smart glasses with BCI are unobtrusively controlled by the user without any gestures or body movements [4].

Hand tracking technology uses tracked images of a user's hand and applies machine learning techniques to estimate important information such as the size, shape, and location of a user's hand and fingers [4]. The hand and body movements of the user can give insights into the user's behavioral biometrics. Data collected in the process is used to authenticate and identify users, which leads to the development of secure and adaptive user interfaces for virtual reality.

Biometric data tracking supplements sensor data collection in VR devices and provides an extensive immersive experience to the users. XR experiences can be tailored with real-time data collection and the application of machine learning algorithms to suit the users. Example: HP Omnicept, which supports training, well-being, creation, and collaboration in XR. The device offers XR experiences driven by human insights and cognitive load [9]. Users' natural responses build their immersive experience at the moment and enable them to discover actionable insights that can take learning, well-being, creation, and collaboration to the next level. Biometric tracking in XR devices measures the cognitive load of the user. It empowers companies that offer virtual training to build applications specific for training by understanding the internal productivity and users' decision-making skills. By delivering an experience that requires expertise, a team under training is prepared to deal with a high-risk situation. It allows the creation of experiences that maximize productivity and diminish development time. A VR app tracks user engagement and assesses user responses at any moment as the face camera allows the users to deliver avatars with genuine facial articulations.VR applications use real-time insights to enhance well-being by extending experiences that relieve

stress, assist, and improve comfort .

VR devices capture the biometric data and assess the cognitive load. Cognitive load defines the amount of brain power exerted by a user for a given task. Psychological researchers suggest that effective cognitive load results in higher information retention, lesser exhaustion, and joy in performing tasks. When cognitive load and performance are optimal, a ”Goldilocks zone” is reached. When users are in this zone, they remain energized and engaged and can complete their tasks comfortably. A low cognitive load often leads to poor performance because tasks become too easy and boring. If the cognitive load is too high, performance suffers because the user is mentally overloaded. XR experiences are refined and tailored for the users by utilizing their brain power .

The ability of XR technologies to gauge the user behaviours and emotional states through biometric tracking has several positive outcomes along with creating a fully immersive experience such as:

1) Compliance: It involves ensuring that the particular group of people are completing their essential activities such as therapy or training [4].Biometric data collection such as eye movement, blood pressure, heart rate enable to understand if a user is experiencing an anxiety, fatigue or any other difficulty in performing the tasks. Adaptive experience enables the users to relax and continue their training or therapies and successfully completing them.
2) Security and Safety: Ensuring that only designated or authenticated users have the access to specific content. It involves ensuring that immersive experiences are in alignment with user's capabilities and needs [4]. User body movements including hand gestures, head movement, alignment in physical space while performing an action contribute to recognizing or authenticating a unique individual. User recognition and procurement of user-specific experience is possible.
3) Usability: It ensures adjusting virtual content and delivery based on how well the user engages with it which enables the content to be made more usable and easily accessible for all the users[4]. Eye tracking and gaze tracking technologies can deduce the personal interests of the user through the eye movement and pupil size dilation during the virtual experience. This information can be used to show the user customized advertisements related to that product or object. The reactions in virtual space can be used to deliver real time experience in physical world.
4) Healthcare: This encompasses individual assessments, treatment, care and therapeutic development, diagnosis, and stress management[4]. Eye movement, pupil size, heart rate, blood pressure, body movements, gestures, respiration rate and other sensitive information about an individual provides an insight into the user's well being both mental and physical states. Figure 3 gives an overview of the health conditions that can be identified using biometric data extracted from ocular, gait, face and voice. Eye tracking technologies are capable of recognizing brain disorders in the user. The information collected during an immersive experience can aid healthcare for the users.

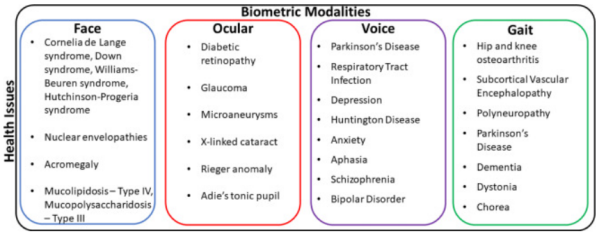

Fig. 3. Health conditions that can be identified using biometrics[10]

5) Personalised digital health coaching: It involves creating digital projections of user's future self to assist them through tough times or challenges in health [4].

III. Biometrically Inferred Data and User Privacy

VR raises some concerns about user privacy. Privacy threats are classified as Physical, Associative, and Informational [11] as viewed in Figure 4. A broad overview concerning privacy is viewed along with subcategories and related circumstances that cause privacy threats. We focus on privacy issues related to biometrics.

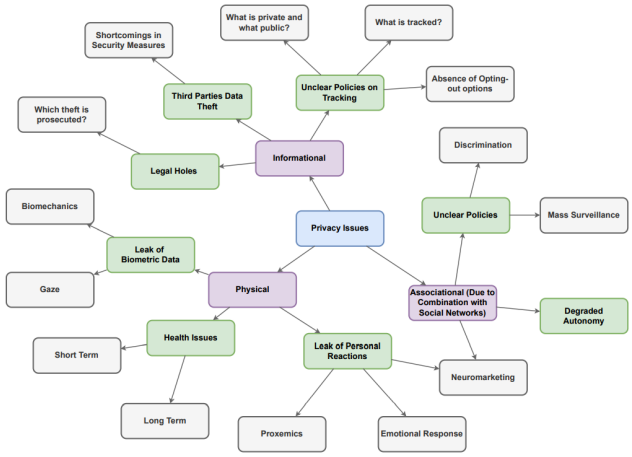

Fig. 4. Privacy related issues in Virtual Reality [11]

Biometrically-inferred data is capable of identifying unique physiological and behavioral characteristics. Biometric data is highly personalized information. Iris scanning, finger scanning, and face and voice recognition techniques find uses for security and authentication in almost every domain that uses intelligent products. Biometrically inferred data gives insights about users' health, age, gender, mental health, cultural background, cognitive processes, and details about many

other sensitive domains seen in Figure 5. While capturing and analyzing patterns in biometrics provides surprising insights, there are also many risks associated with biometrics that could be used against us. An ethical dilemma with biometrics is determining how much of the technology should be considered temporary or unregistered and how much should be allowed. It makes an incomplete attempt to quantify emotional states for various stimuli that come as part of our permanent record.[12].

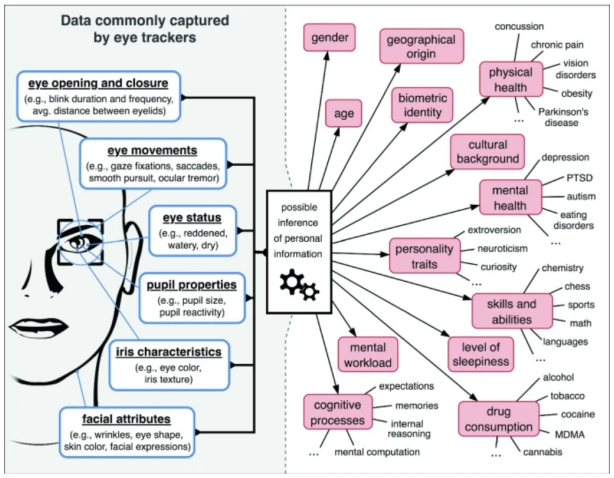

Fig. 5. Biometrically inferred data through eye tracking can reveal a lot of personal information[13]

Eye tracking is a technology that measures a person's eye movements by observing where a person is looking at a given moment and how the eyes move from one place to another. As we study visual information, some information breaks, and others unfold. Our eyes and gaze through an immersive experience show a map of cognitive processes[14]. Figure 5 gives an overview of the biometrically inferred through gaze tracking.

XR technologies are not the only ones collecting and using biometric data of the users. Almost every device with an intelligent framework uses biometric data. Most smartphones and other smart devices use finger scanning, face recognition, or voice recognition to authenticate a user to use the device. Vaults and safes in banks incorporate iris scanning, hand scanning, and other biometric measures to ensure that only verified users have access to their premises. The biometric data collected and used by these institutions is substantially different than its usage in XR technologies. Any biometric data collected on smart devices such as phones or computers is for usage in the physical world. The data collected does not infer information about the user's background, age, sickness, or any personal information to others. Fingerprint scans or voice commands are fed into devices and secure user privacy. These technologies do not utilize the biometric data as the state of art XR technologies do.

Biometric data collected by XR technologies are capable of user recognition using body movements, eye tracking, neural signals, and cognitive load. Behavioral biometrics are determined by tracking user body movement in virtual reality. The data about the user's identification and behavioral patterns are collected without the user communicating. While a user is experiencing an immersive virtual reality, sensitive personal information about them is unconsciously collected. If the user's position data collected by sensors and the biometric data are combined and processed, it enables the identification of the users in a virtual environment. An experiment with physical activities such as bowling and archery in a virtual environment illustrates that an individual performing the task is identifiable using spatial data and body movements[16]. Users who perform tasks in virtual reality are identified [16] based on their body movements. [17] concludes user identification through tasks like pointing, grabbing, typing, and walking in a group of users.

An immersive XR experience has the potential to unlock the user's physical location, age, race, gender, and other thoughts and interests without the user's consent or knowledge, as Figure 5 describes. When coupled, spatial motion data with eye-tracking techniques, user identification, and behavioral and mental traits determination are possible. XR technologies fully or partially capture all user data in an unconscious and un-communicated manner to replicate the user behavior in virtual space. User names should be suppressed, and the generalization method should be applied to the age and region of the users to maintain privacy. Other sensitive information, such as gender, should be flagged as such to inform them about the risk of privacy.[18].

XR technologies might use the data to improve their product and provide a better experience to users, but not all users are comfortable sharing their data [15]. Figure 5 demonstrates personal attributes identifiable using eye-tracking data. User viewpoint could be analyzed using a survey that would collect user responses and demonstrate user privacy concerns about using eye-tracking data [15]. Users respond to questions about VR technologies, eye-tracking, data sharing, and if they are willing to share their data collected by eye-tracking [15]. In the first part, the survey presents currently available services, options to be adopted, and if they would trust these services with their eye-tracking data. People were willing to share personal attributes such as race, identity, gender, age, mood and emotions, and sexual preferences. They approve data use for disease detection, reading skill improvement, learning skill development, stress level monitoring, and natural virtual reality interaction [15] as seen in Figure 6. Users respond to questions regarding sharing their eye-tracking data in general. As seen in Figure 7, people would share their eye-tracking data to different products/businesses or legal usages. These institutions include government, health, and local or international companies. They approve data to use in internal company matters. Users feel secure sharing data with research institutes in a public, private, or constrained environment in exchange for benefits or VR/AR usage [15].

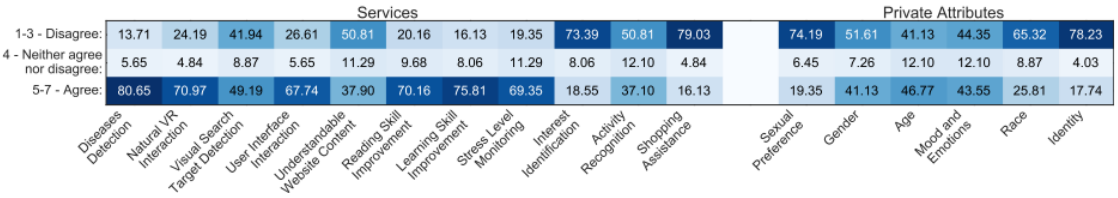

Fig. 6. Survey results depicting if users are comfortable sharing their personal data for sectors[15].

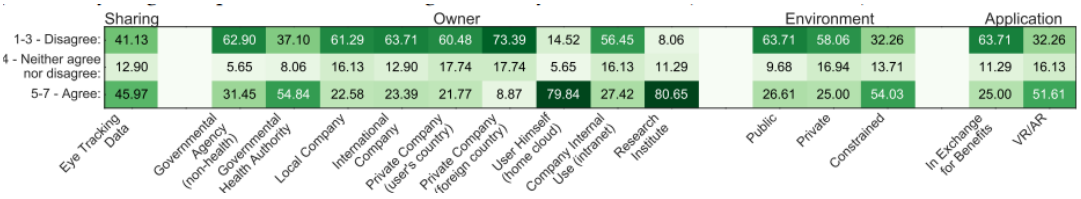

Fig. 7. Survey results depicting if people would share their eye tracking data with an owner in return for VR exchange[15].

With all the biometrically inferred data, third parties can model a digital twin of a user in the virtual environment, that is, a virtual avatar with realistic expressions, attitudes, thoughts, and preferences, and with the user's appearance in the real world. Avatars play a crucial role in the virtual world. It represents the user's physical self and allows them to experience the adventures and activities of the virtual world through their creation, manipulation and customization. Virtual avatars display unique behaviors, intentions, and styles that are identical to real-world users[19]. Users may be blackmailed or threatened once their preferences and interests are derived. Internet-connected physical and virtual worlds hold a lot of scope for privacy and security violation. The actions, movements, and gaze analysis of the digital twin of a user might be resourceful in gathering information about the user's brain power and cognitive and thinking capability. When devices capture neural signals of the user's brain, it affects the physical and mental privacy of the user [5]. Immersive virtual twin models of the users restrict them from navigating virtual environments in anonymity.

Biometric data accounts for user individuality and uniqueness. Using biometric data to create realistic twin models in virtual space jeopardizes user privacy. Researchers at Stanford claim that about 20 million body languages of the users can be generated in 20 minutes of an immersive experience [4]. XR experiences gauge users' subconscious and reveal their interests in food or sexual orientation. It breaches user autonomy and anonymity. XR devices should be developed under data protection and privacy protocols so that users can trust the system. Laws and regulations concerning data protection should be abided by the companies manufacturing devices or the companies that collect user data. A VR device, HP Omnicept, procures adaptive experiences using cognitive load following General Data Protection Regulation (GDPR). Users should know that data specific to them would be collected but would remain confidential. Although XR devices need biometric data to provide an intensive and immensely immersive experience, it forms the core functionality of the technology users should be aware of data collection and the autonomy to decide about it.

IV. Privacy Concerns in XR

A. Existing limitations and approaches to improve mitigation practices:

Due to the immersive nature of user data collection in AR/VR, many of the standard mitigation approaches used to mitigate the damage caused by different types of data are insufficient in the context of these experiences [4]. User-centric consent, transparency, and disclosure measures are more complex in AR/VR than in other digital and connected technologies. Unlike two-dimensional platforms, users fully or partially interact with virtual spaces, which may require reworking standard consent procedures for an immersive experience[4]. Users may not be able to easily click hyperlinks to additional information or consent to a fully immersive experience. Users who prefer privacy can also choose not to share or publish certain information. This approach has significant limitations because the core functions of immersive technologies require sensitive or potentially identifiable data [4].

XR stakeholders should actively develop or support efforts to standardize differential privacy or other privacy protocols that protect individual identities and data[5]. XR developers must consider which sensitive personal data can be processed locally and stored on the device. It must be ensured that sensitive personal data is encrypted in transit and remains inactive. XR platforms and experience providers must implement virtual identity and ownership rules that reduce, rather than increase, online harassment, digital vandalism, and fraud. They should have clear guidelines limiting physical risks to XR users and bystanders. Policymakers should consider how existing or proposed data protection laws can give consumers meaningful rights and businesses clear obligations regarding XR data.

B. Regulations for User Privacy:

The General Data Protection Regulation (GDPR) aims to empower data privacy for all users in EU [20]. The General Data Protection Regulation (GDPR) applies to all organizations that store and process personal information in the European Union, regardless of location[20]. Regulations for collecting biometric data as per the GDPR framework impose the following:

1) Consent: Data processing is only lawful if the interested party authorizes the personal data for one or more declared purposes. The operator must indicate that a user has given consent to data processing, and it could be withdrawn at any time if they decide to do so. [20].
2) Freely given: If the user consents to use personal details in the contract and if it is not necessary for the performance of the contract, the consent is not considered freely given.[20].
3) The record of processing actions: The data controller has a positive obligation to maintain a written record of the data collected, including:
   (a) The purpose for which data is collected
   (b) Categories of data subjects and a description of the personal data
   (c) Categories of recipients and personal information are provided, general description of the technical and organizational security measures that the operator has taken or has been made public or will be disclosed [20].
4) Appointment of a representative: All controllers outside the EU have the right to act on their behalf unless the group is accidental and could endanger the rights and freedoms of individuals given its nature and circumstances. The scope of processing should be specified exclusively, even if it is by an authority, public body or the manager[20].
5) Notification period of 72 hours: All operators must notify the supervisory authority within 72 hours of receiving notification of a personal data breach [20].

C. Privacy aware method for collecting biometric data:

Along with the legal protocols to secure user biometric data, adopting privacy-aware techniques when user experiences XR is crucial. Biometric data collected from eye-tracking allow the other parties to know a user and his traits without their consent. As eye tracking is increasingly integrated into virtual and augmented reality (VR / AR) head-mounted displays, preserving user privacy is becoming an increasingly important aspect [15].A method to safeguard user privacy by preventing re-identification of users or revealing their gender information is differential privacy [15]. One of the biggest challenges of differential privacy is finding the trade-off between privacy and convenience. In other words, finding the right amount of random noise to ”hide” people without losing the usefulness of the data [15]. The mechanism would prevent realistic projections of behavioral traits in the virtual space. Differential privacy prevents third parties, such as companies or hackers, from extracting personal characteristics from eye movement while maintaining the usefulness of data for non-personal data [15]. Gathered data would be able to determine meaningful insights about user experience and feelings but would not potentially identify the user and misuse their identity. Differential data protection ensures that the response of the data protection mechanism does not depend on whether an individual user provided their data or not; Therefore, no further information about the user could be derived.

V. Limitations and Future Scope

Anonymizing data is tricky, given the number of user-provided and user-generated identifiers. Even if the tracking data is anonymized by removing the name, raw biometric data can relatively re-identify a user based on their unique movements with ease[4]. Simply removing usernames would not help. Additional techniques are required to anonymize sensitive and biometric-derived data[4]. Therefore, secure storage and clear access restrictions become particularly important, which raises questions about the benefits and risks of different data management approaches. The most significant aspect to consider is whether users or third parties can access their data and whether sufficient data security measures are in place.[4]. Existing legal safeguards may not be adequate to address the risks of various data collected from AR/VR systems[4]. It is similar to laws that aim to prevent non-consensual pornography but fail to protect users from having their anonymity and autonomy violated by virtual copies or virtual assets of themselves. This political divide is reflected in the proliferation of deep fakes and synthetic media that reproduce the image of individuals, raising concerns about individual autonomy and the right to publish digital copies.[4]. However, the risk is even greater for immersive experiences that may not require the technical complexity of synthetic environments. Example - An unauthorized user gains access to another user or controls another user’s virtual existence (for example, by logging into an individual user account), impersonating the user, or impersonating the user without permission, acting, or speaking.[4]. Malicious actors can also impersonate virtual entities without such unauthorized access. With enough traceable information, avatars and other virtual assets can be cloned. It is not difficult to imagine such clones being used in fraudulent practices, causing emotional, reputational, and economic damage[4].

XR platforms should try to adopt voluntary proposals such as ”Neuro Rights” to ensure that users’ intellectual privacy is not violated. They must disclose (in plain language) and allow users to decide what personal data is collected, how this data is processed, for what purposes, and for how long it (and its processed results) is retained. Individuals should have the right to choose how their identity (or its representations/modifications, such as digital twins or enhanced appearances) is viewed and appropriated by others in XR[5]. The New European Bauhaus initiative states that measures are taken to secure the privacy of digital twins and mitigation principles are adopted such that the innovation retains customer trust.

VI. Conclusion

AR and VR technologies are not transitory trends that fade. XR has made notable technological advances. It has emerged as the greatest fascination for displaying holographic views, augmented objects, VR movies, and real-time adaptive VR experiences. Creating user-tailored experiences requires collecting as much user-specific data as possible. Attributes unique to the user allow real-time customization. User biometric data preservation is crucial for every company that creates or develops XR. There are many laws and regulations to secure biometrics. As courts push their way into biometric privacy cases, the requirements and impact of these regulations will become impactful globally. AR and VR companies should consider the location of their consumers and adapt their operations accordingly. Evaluating companies' risk tolerance against their desire to use biometrics in light of the growing body of state law is critical to help XR stakeholders make business decisions. Therefore, XR stakeholders and developers should adopt responsible measures to deliver a cutting-edge XR experience.

Acknowledgment

. I wish to thank my supervisor for feedback and support while working on this report.

References

[1] S. Al-saleh, "Personal identification in virtual and augmented reality: Control systems perspective."

[2] N. Shadowen and D. Hosfelt, "Addressing the privacy implications of mixed reality: A regulatory approach," *arXiv preprint arXiv:2007.10246*, 2020.

[3] C. Andrews, M. K. Southworth, J. N. Silva, and J. R. Silva, "Extended reality in medical practice," *Current treatment options in cardiovascular medicine*, vol. 21, no. 4, pp. 1–12, 2019.

[4] N. Morris, ""an imperative developing standards for safety and security in xr environments",xrsi.org," 2021.

[5] McGill and Mark, "The ieee global initiative on ethics of extended reality (xr) report–extended reality (xr) and the erosion of anonymity and privacy," *Extended Reality (XR) and the Erosion of Anonymity and Privacy - White Paper*, pp. 1–24, 2021.

[6] Y. Pan and A. Steed, "The impact of self-avatars on trust and collaboration in shared virtual environments," *PloS one*, vol. 12, no. 12, p. e0189078, 2017.

[7] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, and B. Gordijn, "The convergence of virtual reality and social networks: threats to privacy and autonomy," *Science and engineering ethics*, vol. 22, no. 1, pp. 1–29, 2016.

[8] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," *International Journal of Applied Engineering Research*, vol. 13, no. 5, pp. 2276–2297, 2018.

[9] E. Siegel, J. Wei, A. Gomes, M. Oliviera, P. Sundaramoorthy, K. Smathers, M. Vankipuram, S. Ghosh, H. Horii, J. Bailenson *et al.*, "Hp omnicept cognitive load database (hpo-cld)–developing a multimodal inference engine for detecting real-time mental workload in vr," Technical report, HP Labs, Palo Alto, Tech. Rep., 2021.

[10] A. Ross, S. Banerjee, and A. Chowdhury, "Deducing health cues from biometric data," *Computer Vision and Image Understanding*, p. 103438, 2022.

[11] A. Giaretta, "Security and privacy in virtual reality–a literature survey," *arXiv preprint arXiv:2205.00208*, 2022.

[12] K. Bye, D. Hosfelt, S. Chase, M. Miesnieks, and T. Beck, "The ethical and privacy implications of mixed reality," in *ACM SIGGRAPH 2019 Panels*, 2019, pp. 1–2.

[13] J. L. Kröger, O. H.-M. Lutz, and F. Müller, "What does your gaze reveal about you? on the privacy implications of eye tracking," in *IFIP International Summer School on Privacy and Identity Management*. Springer, 2019, pp. 226–241.

[14] D. Hosfelt and N. Shadowen, "Privacy implications of eye tracking in mixed reality," *arXiv preprint arXiv:2007.10235*, 2020.

[15] J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling, "Privacy-aware eye tracking using differential privacy," in *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*, 2019, pp. 1–9.

[16] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass, "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–11.

[17] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek, and F. Alt, "Behavioural biometrics in vr: Identifying people from body motion and relations in virtual reality," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[18] A. Tepljakov and H. Bahsi, "User behavior analysis for predictive virtual reality applications: An ethical and data security perspective," 2020.

[19] G. Freeman, S. Zamanifard, D. Maloney, and A. Adkins, "My body, my avatar: How people perceive their avatars in social virtual reality," in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–8.

[20] E. K. . A. Bedat. (2018) Virtual reality, augmented reality & biometric data after 2017. [Online]. Available: https://blog.klarislaw.com/vr-ar-virtual-reality-augmented-reality-biometric-data-after-2017-ed-klaris-alexia-bedat-a15e9cb000a1