Brittan Heller
June 4, 2022
Submission to OHCHR

Privacy and the Metaverse
Prepared for the United Nations High Commissioner for Human Rights

This submission identifies recent trends and challenges with regard to human rights and the metaverse, specifically focusing on privacy and related principles, safeguards and recommendations, for the OHCHR report to the Human Rights Council at its fifty-first session.[1]

What is the Metaverse?

The right to privacy is paramount when it relates to immersive technologies, in particular augmented reality (AR) and virtual reality (VR), collectively known as mixed reality (XR) or the metaverse.[2]

Understanding how XR technology works is essential to understanding the unique privacy risks that the technology poses. XR users say the technology is a window into another world. VR is an interface worn on the body that places users inside an interactive virtual environment.[i] Putting on a head-mounted device (HMD) allows the user to experience the sights and sounds of a digital alternative universe.[ii]

AR can be defined as an interface that layers digital content on a user's visual plane.[iii] AR is often accessed through glasses or a smartphone.[iv] Rather than transporting the user to a new world, AR enables users to enrich the world they inhabit.

XR combines VR and AR experiences, displaying elements of virtual and actual environments together and sometimes switching between them.[v] New VR-web browser combinations are crossing lines between the internet and VR usage, raising expectations for further medium-spanning integrations.[vi]

In other words, XR is the next pervasive spatial computing network, operating via sensors, and containing features designed to replace your smartphone.

---

[1] Brittan Heller is an attorney specializing in technology and human rights. She is a fellow at the Atlantic Council's Digital Forensics Research Lab. She was an inaugural Technology and AI Fellow at Harvard Kennedy School, studying human rights and immersive worlds. Heller previously practiced at the U.S. Department of Justice, the International Criminal Court, and Foley Hoag LLP. She is a board member at the Virtual World Society, a member of the World Economic Forum's Steering Committee for Metaverse Governance, and a term member of the Council on Foreign Relations. She is graduate of Yale Law School and Stanford University.

[2] Research summarized from Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VANDERBILT LAW REVIEW 1 (2021), https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1; *see also* Brittan Heller, *Reimagining Reality: Human Rights and Immersive Technology*, Carr Center Discussion Paper Series, 2020-008 (2020), https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf.

Benefits of XR

Proponents of immersive technologies point to the transformational power of the medium. The experience of being in a XR environment for the first time is like stepping into a new world, where the program and hardware create a digital blank slate for experience. Simply put, it feels real.

More specifically, the magic of the XR medium is characterized by the existence of immersion – the user feeling as if they are actually in the virtual world; presence – the user experiencing the virtual world as real; and embodiment – the user appearing as an avatar and treating its experiences as their own.[vii] This creates incredible opportunities for medicine, increased human connection, augmented empathy, enterprise usage, and new educational opportunities.[viii]

Privacy Implications of XR

However, XR presents complex privacy issues because of the anatomical measurements and the sensors needed to position users in space – and inferences about one's preferences, veracity, emotions or state of mind, along with their physical or mental health, that can be made from the data.

An immersive system must understand how users interact with the world at a foundational level. HMDs and smartglasses use a system of cameras and sensors to track and respond to the user's eyes, movements, and gestures.[ix] If it does not do this, users can experience nausea and disorientation, and the experience will lack immersion. As part of this, immersive systems use eye-tracking to gauge what the user looks at and for how long.[x] XR implicitly tracks how individuals react to stimuli – do they stare? Do they resolutely look away? How do their pupils respond to the experience? Does their heart rate increase?[xi] These are involuntary behaviors that humans do as naturally and thoughtlessly as breathing. This data can be deeply revealing about who people fundamentally are, but an XR system must process this information to effectively deliver its benefits.

Potential Harms from XR

Critics caution against unfettered optimism, and focus on the opportunities for misuse and abuse, like harassment and violations of consumer privacy. Traditional social harms that have manifested on the internet, such as harassment or threats of violence, land with stunning force in immersive systems. This is because of neuroscience. The brain processes digital world experiences in XR in the same way that memories are formed, through the hippocampus. From the vantage point of the user's brain, what happens in XR is an actual reality. Psychological realness also causes immersive technology users to physiologically respond to virtual simulations in ways that are similar to their bodily responses to real situations.[xii] It follows that

the recent uptick in reports of sexual harassment of women and targeting of minorities in XR actually feel like a tangible assault to the victims.

A New Privacy Harm: Biometric Psychography

Immersive technology poses inherent risks, which our legal understanding of privacy, biometrics, and online harms is simply not prepared to address. As a 2019-2020 Technology and AI Fellow at the Harvard Kennedy School, the author proposed a new area of legal and policy inquiry raised by immersive technology called "biometric psychography."

Biometric psychography is a new concept for a type of bodily-centered information that can reveal intimate details about users' likes, dislikes, preferences, and interests. XR technology must capture this data to function, meaning that while biometric psychography may be relevant beyond AR and VR, it will become increasingly inescapable as the technology spreads. This is important because current thinking around biometrics is focused primarily on identity, but biometric psychography is the practice of using biometric data to instead identify a person's thoughts and interests.[xiii]

Biometric psychography uses behavioral and anatomical information (e.g., pupil dilation) to measure a person's reaction to stimuli over time. This can reveal both a person's physical, mental, and emotional state, and the stimuli that caused them to enter that state. It is a combination of biometrics and psychographic information, which is a term adopted from advertising that refers to metrics that evaluate a consumer's activities, interests, and opinions through their cognitive attributes, like emotions, values, and attitudes.[xiv]

To illustrate the distinction, think of traditional biometrics like static images of fingerprint swirls that connect an individual to their unique personhood and identity; psychographics, on the other hand, are more akin to consumer profiles that map an individual's buying preferences or shifts in opinion over time. This difference is important because of the character and implications of the information that could be included as biometric psychographics. Although limited, there is law that regulates traditional identity-focused biometrics and scholarship focusing on its impacts.[xv] But there is no law, as of yet, on the implications of biometric psychography.

XR technology can measure biometric information and retain data far beyond the law's focus on biometric identifiers.[xvi] It is not limited to static measurements or images because sensors track how users move over a period of time.[xvii] Furthermore, it constantly records changes in the environment and how that change may impact the user's condition over time.[xviii] It is not just the user's real identity, which is mostly already known by the XR platforms from their financial information and verifiable account information. Instead, it is a new quality of information that is comprised of the user's real identity combined with their reactions to particular stimuli—indicating what someone uniquely may think and like and want.[xix]

What type of information would be included as part of biometric psychographics? One part is biological info that may be classified as biometric information or biometric identifiers.[xx] Looking

to XR technology, the following are biometric tracking techniques: (1) eye tracking and pupil response;[xxi] (2) facial scans;[xxii] (3) galvanic skin response;[xxiii] (4) electroencephalography (EEG);[xxiv] (5) electromyography (EMG);[xxv] and (6) electrocardiography (ECG).[xxvi] These measurements tell much more than they may indicate on the surface. For example, facial tracking can be used to predict how and when a user experiences their emotions.[xxvii] It can trace indications of the seven emotions that are highly correlated with certain muscle movements in the face: anger, surprise, fear, joy, sadness, contempt, and disgust.[xxviii] EEG shows brain waves, which can reveal states of mind.[xxix] EEG can also indicate one's cognitive load.[xxx] How aversive or repetitive is a particular task? How challenging is a particular cognitive task?[xxxi] Galvanic skin response shows how intensely a user may feel an emotion, like anxiety or stress, and is used in lie detector tests.[xxxii] EMG senses how tense a user's muscles are and can detect involuntary micro-expressions, which are useful in detecting whether or not people are telling the truth (since telling a lie would require faking involuntary reactions).[xxxiii] ECG can similarly indicate truthfulness, by seeing if one's pulse or blood pressure increases in response to stimuli.[xxxiv]

Furthermore, pupil dilation measurements can be used to ascertain a frightening range of personal information, like to whom a user is sexually attracted or whether a user may have a propensity for developing illnesses.[xxxv] HMDs that include eye-tracking capabilities can gauge what their users are looking at, how long their attention is captured, and how users may feel about what they are seeing, allowing advertisers to collect data that used to require a laboratory.[xxxvi] This "mind reading" capability, which is becoming a standard feature in new HMDs, may change the fundamental nature of the technology and put users on guard for self-censorship of their innermost thoughts, feelings, and emotions.

It is important to note that biometric psychography is not limited to immersive technology. Video gait analysis is used to assess emotional states, and a range of similar applications may arise as technology evolves.[xxxvii] However, data that enable biometric psychography *must* be captured for immersive technology to function,[xxxviii] which means this field will likely grow as XR technology expands.

How Could Biometric Psychography Implicate Privacy?

The combination of data sets inherent in XR technology may produce further invasive results that amount to more than a violation of consumer privacy – pupillometry offers the perfect illustration of this risk. Many people are surprised by how much can be revealed through evaluating the motions of the eye, like examining saccades, the scanning motions that eyes use to create a picture of the world, or "smooth pursuit" motions made by the eye in tracking a moving object.[xxxix] Some researchers have found that autism in some young children can be gauged by irregular eye motion patterns.[xl] Other serious ailments, like schizophrenia, Parkinson's disease, ADHD, and concussions can also be diagnosed though eye tracking.[xli]

This could have serious implications. For example, scientists in Germany conducted a study asking subjects to complete a maze in VR.[xlii] They found that users' performance on the task was

correlated with their risk of developing Alzheimer's disease.[xliii] Performance on a XR game is not the type of information that lawmakers who created health privacy laws anticipated as related to one's medical health. But access to such information would cause alarm to privacy and consumer advocates, especially if users' results were available for purchase by third parties, like insurers, advertisers, and government agencies.

Previous examples have mentioned how pupil dilation, in particular, can help measure very intimate information like users' innermost thoughts and desires.[xliv] It is frightening to think that companies could sell or use information, like a user's predicted sexual orientation, to enrich existing commercial profiles. There is a risk of self-censorship, in the most fundamental way, if users find themselves trying to limit what they feel, think, or express for fear that information will be monetized or researched. At the same time, many of these factors are subconscious, meaning that even if a user wanted to self-censor or hide their preferences, the user would be unable to.

If third-party developers or direct developers are able to integrate different data sets in ways that are unanticipated or harmful to consumers, this could reveal information that users do not intend – or meaningfully consent – to reveal. This could similarly occur with government or corporate use of XR if the technology was used in interrogations or in contexts like anti-bias and harassment training. Without uniform legal restrictions or voluntary constraints outside of identifying information, which is the focus of current biometrics regimes, there is the potential for companies to be susceptible to another *Cambridge Analytica*-scale violation of user trust.[xlv] Furthermore, it is challenging to inform users of the full implications of collection of their data. Most people do not understand how involuntary bodily indicators of emotional responses, mental state, or health can disclose fundamentally private information, such as truthfulness, inner feelings, and sexual arousal.

A Legal Gap

Data analysis based on insights from biometric psychography could build psychological user profiles based on specific bodily data such as eye tracking, pupil dilation, and other physical analysis.[xlvi] Importantly, while much of the data that would enable this work seems intuitively similar to biometric data, it is generally excluded from existing legal definitions, leaving a large and growing regulatory gap.[xlvii]

Many privacy laws around the world do not accommodate the functions and features of this new spatial computing hardware. The laws are centered around concepts of personal identifying information, but in XR, the issue is different. It is more akin to mental privacy or neurorights regimes, protecting inferences that can be made from our involuntary reactions to stimuli.

Marrying traditional biometrics and predictive behavioral analytics is a nascent discipline, newly possible because of technological advances.[xlviii] There are currently no strong legal safeguards in the United States, where most XR companies are incorporated, on the use, sale, gathering, and

storage of this type of information. It is not readily covered under existing biometrics law.[xlix] While not unique to XR,[l] biometric psychography is uniquely suited to this new industry, evolving from ads-based social media, that is looking for ways to make XR into a popular and profitable enterprise.[li]

Potential Mitigations

Because of the psychological aspects that make XR immersive, and the potential for negative impacts on individual users and their communities, the author argues that we should examine immersive media through a human rights-oriented lens. A human rights-based framework would integrate human dignity into the foundation of XR systems, just like privacy-by-design frameworks foreground privacy-related concerns at the onset of product and policy development.

Specifically, a human rights lens would mean that immersive creators and lawmakers should examine mismatches between existing privacy law and new forms of potential safety violations that implicate the fundamental rights of users – along with examining nascent risks inherent in both the interfaces and the XR content itself.

Furthermore, States and international organizations should press XR companies on their business models and issue regulations. One baseline recommendation could be a prohibition on biometric psychography in XR, because of the inability to meaningfully consent to the monetization of one's involuntary bodily responses. Another could be the promotion of a new concept of mental privacy, to expand the phenomenon of privacy beyond identity. Because of the unique psychological and physiological aspects of XR, and the potential for a new invasive class of privacy-related harms, OHCHR could be vocal about the need for increased caution to protect users. This will help guide the nascent XR industry in an evolving human rights landscape and ensure that the beneficial uses of this powerful technology outweigh the potential misuses.

To take a human rights-based approach to XR technology, OHCHR could ask questions like: What risks emerge from the capabilities being built as standard features into typical VR and AR hardware? What risks of user abuse or violations of the right to freedom of expression, freedom of assembly, and safety of users can be reasonably anticipated? Will targeted advertising, via biometric psychography, be permitted? What does content moderation look like in an immersive environment? How does enforcement of content moderation work? Do we need to reconceive of privacy risks in the XR context? Given these inquires, what sort of actions can we take today to preserve human rights in virtual spaces?

Examining these fundamental questions at a formative stage in the lifecycle of XR technologies – when the hardware is still not solidified and mass adoption is on the cusp – may help stave off some of the pitfalls that global communities have experienced in the other forms of internet-based technologies, and may give us the opportunity to apply this new powerful medium in socially affirming and personally beneficial ways.

i. Joe Bardi, *What is Virtual Reality? [Definition and Examples]*, MARXENT 3D COM., https://www.marxentlabs.com/what-is-virtual-reality/.

ii. *Id.*

iii. Kevin Bonsor & Nathan Chandler, *How Augmented Reality Works*, HOW STUFF WORKS, https://computer.howstuffworks.com/augmented-reality.htm.

iv. *See id.*

v. *Id.*

vi. *See, e.g.*, MOZILLA MIXED REALITY, https://mixedreality.mozilla.org.

vii. *See* Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VANDERBILT LAW REVIEW 1 (2021), at Section III.B.2.

viii Virtual World Society, VIRTUAL WORLD SOCIETY, https://www.virtualworldsociety.org (last visited Dec 31, 2019). The Virtual World Society exist to promote affirming uses of new immersive technology to benefit humanity, with a particular focus on improving the lives of children.

ix. *Head-Mounted Displays (HMDs)*, VIRTUAL REALITY SOC'Y, https://www.vrs.org.uk/virtual-reality-gear/head-mounted-displays.

x. *See* Heller, *supra* note vii, at Section III.A.1.

xi. *Id*.

xii. JEREMY BAILENSON, EXPERIENCE ON DEMAND: WHAT VIRTUAL REALITY IS, HOW IT WORKS, AND WHAT IT CAN DO 14–17 (2018), at 28.

xiii. *Compare Biometrics*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biometrics (focusing on biometrics as a means to verify identity), *with* Ali Fenwick, *Psychographics: How Big Data Is Watching You*, HULT: BLOGS, https://www.hult.edu/blog/psychographics-big-data-watching (focusing on the shift to identifying interests).

xiv. *See Psychographics*, BUS. DICTIONARY, http://www.businessdictionary.com/definition/ psychographics. html.

xv. Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, ANTITRUST, Summer 2017, at 60, 62–64 https://www.robinskaplan.com/-/media/pdfs/the-future-is-now-biometric-information-and-data-privacy.pdf.

xvi. *Compare id.* (discussing various state laws that define "biometric identifiers" to be retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, vein scans, or other physical characteristics), *with* DIANE HOSFELT, MAKING ETHICAL DECISIONS FOR THE IMMERSIVE WEB 2 (May 14, 2019), https://arxiv.org/pdf/1905.06995.pdf (explaining that immersive technology can measure a user's sexual attraction or sexual orientation through pupil dilation and skin temperature and can determine whether or not someone is a high or low performer though facial movement data during tasks).

xvii. *See id.* (explaining that immersive technology sensors collect data such as pupil dilation and facial movements).

xviii. *See* Alexandra Kitson, Mirjana Prpa & Bernhard E. Riecke, *Immersive Interactive Technologies for Positive Change: A Scoping Review and Design Considerations*, FRONTIERS PSYCH. 14–15 (Aug. 8, 2018), https://www.frontiersin.org/articles/10.3389/fpsyg.2018.01354/full.

xix. HOSFELT, *supra* note xvi.

xx. Roberg-Perez, *supra* note xv, at 62.

xxi. HOSFELT, *supra* note xvi.

xxii. Kent Bye, *#517: Biometric Data Streams & the Unknown Ethical Threshold of Predicting & Controlling Behavior,* VOICES VR PODCAST (Mar. 20, 2017), http://voicesofvr.com/517-biometric-data-streams-the-unknown-ethical-threshold-of- predicting-controlling-behavior/.

xxiii. *Id.* Galvanic skin responses is a change in the electrical resistance of the skin caused by emotional stress, measurable with a sensitive galvanometer. Egert Teesaar, *Background: Lie Detection*, MEDIUM (Dec. 17, 2019), https://medium.com/lie-detector-from-emg/background-344e625b2d1. It is used in lie-detector tests. *Id.*

xxiv. *See* Alexandra Kitson, Mirjana Prpa & Bernhard E. Riecke, *Immersive Interactive Technologies for Positive Change: A Scoping Review and Design Considerations*, FRONTIERS PSYCH. 14–15 (Aug. 8, 2018), https://www.frontiersin.org/articles/10.3389/fpsyg.2018.01354/full, at 12–13.

xxv. Kent Bye, *#814: Neuroscience & VR: Using Muscles & EMG for Neural Interfaces with CTRL-Labs,* VOICES VR PODCAST (Sept. 12, 2019), https://voicesofvr.com/814-neuroscience-vr-using-muscles-emg-for-neural-interfaces-with-ctrl-labs.

xxvi. Bye, *supra* note xxii.
xxvii. HOSFELT, *supra* note xvi.
xxviii. Bye, *supra* note xxii.
xxix. *Id.*
xxx. *Id.*
xxxi. *Id.*
xxxii. *Id.*
xxxiii. *See id.*; *see also* Egert Teesaar, *Background: Lie Detection*, MEDIUM (Dec. 17, 2019), https://medium.com/lie-detector-from-emg/background-344e625b2d1f.
xxxiv. *See* Bye, *supra* note 2xxii *see also* Runxin Yu, Si Jia Wu, Audrey Huang, Nathan Gold, Huaziong Huang, Genyue Fu, & Kang Lee, *Using Polygraph to Detect Passengers Carrying Illegal Items*, 10 FRONTIERS PSYCH. 322 (Feb. 25, 2019), https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00322/full.
xxxv. Interview with Kent Bye, Host, Voices of VR Podcast, in Portland, Or. (July 22, 20190).
xxxvi. Avi Bar-Zeev, *The Eyes Are the= Prize: Eye-Tracking Technology Is Advertising's Holy Grail*, VICE (May 28, 2019), https://www.vice.com/en_us/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail.
xxxvii. *See* Matt Simon, *This Robot Can Guess How You're Feeling by the Way You Walk*, WIRED (May 18, 2020), https://www.wired.com/story/proxemo-robot-guesses-emotion-from-walking/.
xxxviii. *See* Bye, *supra* note xxii.
xxxix. *See id.*
xl. *Id.*
xli. *Id.*; *see also* Tia Ghose, *Eye Tracking Could Diagnose Brain Disorders*, LIVE SCI. (Sept. 18, 2012), https://www.livescience.com/23274-eye-tracking-gaze-brain-disorders.html.
xlii. David Shultz, *Alzheimer's Disease Tied to Brain's Navigation Network*, SCIENCE (Oct. 22, 2015), https://www.sciencemag.org/news/2015/10/alzheimer-s-disease-tied-brain-s-navigation-network.
xliii. *Id.*
xliv. Bar-Zeev, *supra* note xxxvi.
xlv. *See* Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram*, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.
xlvi. *See* Hanish Bhatia, *Behavioral Biometrics: The Next Step for User Authentication*, COUNTERPOINT (Feb. 11, 2019), https://www.counterpointresearch.com/behavioral-biometrics-next-step-user-authentication/.
xlvii. *See* Heller, *supra* note vii, at Section IV.A.3.
xlviii. *See, e.g.*, IMOTIONS, https://imotions.com.
xlix. Ed Klaris & Alexia Bedat, *VR & AR: Virtual Reality, Augmented Reality & Biometric Data After 2017*, MEDIUM (Jan. 31, 2018), https://blog.klarislaw.com/vr-ar-virtual-reality-augmented-reality-biometric-data-after-2017-ed-klaris-alexia-bedat-a15e9cb000a1.
l. For an application using gait to attempt to perceive emotion, *see* Matt Simon, *This Robot Can Guess How You're Feeling by the Way You Walk*, WIRED (May 18, 2020), https://www.wired.com/story/proxemo-robot-guesses-emotion-from-walking/.
li. *How Does Eye Tracking Work?*, VR.ORG (Feb. 22, 2018), https://www.vr.org/2018/02/22/how-does-eye-tracking-work/.