Embodied Harms and Inferred Data: Redefining Privacy in Virtual Reality

Sean Balbale

I. INTRODUCTION

The emergence of Extended Reality (XR),[1] an umbrella term for Virtual and Augmented Reality (VR/AR) technologies, represents a paradigm shift in human-computer interaction. Unlike previous digital eras where extensive data collection was technically optional, immersive technologies require the continuous collection of intimate user data to function. This new data-gathering model creates profound ethical and technical challenges. The primary risk is not identification—such as iris or fingerprint scans—but inference. These systems passively collect "behavioural biometrics," including subtle head motions, hand movements, and eye-gaze patterns.[2]

The power of these new data streams is significant; technical analyses demonstrate that VR users can be "uniquely recognised with approximately 90% accuracy using head motions" alone.[3] This data enables platforms to infer sensitive information that individuals did not choose to disclose, including mental and physical health status,[4] sexual preferences,[5] and concentration levels.[6]

Consequently, the locus of data collection moves from an active process (such as clicks or text entries) to a passive one. This Article examines four primary dimensions of this shift: (1) competing architectures of control; (2) the nature of immersive harm; (3) the obsolescence of existing law; and (4) the search for a new governance model. A critical gap persists between voluntary, corporate-led technical solutions and the growing necessity for legally mandated public frameworks.

II. COMPETING ARCHITECTURES OF CONTROL

A fundamental dichotomy exists in the industry regarding the management of this new data stream: server-side surveillance versus on-device privacy. The surveillance capitalism model,[7] pioneered

[1] Extended Reality (XR) is an umbrella term for immersive technologies that blend the physical and virtual worlds. It encompasses the entire spectrum, including Virtual Reality (VR), which fully immerses the user in a digital environment; Augmented Reality (AR), which overlays digital information onto the real world; and Mixed Reality (MR), which allows digital and physical objects to co-exist and interact in real-time.

[2] Dilshani Kumarapeli et al., *Privacy Threats of Behaviour Identity Detection in VR*, 5 FRONTIERS IN VIRTUAL REALITY § 1 (2024).

[3] *Id.* § 2.1.

[4] *Id.* § 2.2.

[5] Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, INFO. TECH. & INNOVATION FOUND. 11 (Mar. 4, 2021) [hereinafter Dick].

[6] Vasilis Xynogalas & M.R. Leiser, *The Metaverse: Searching for Compliance with the General Data Protection Regulation*, 14 INT'L DATA PRIVACY L. 91 (2024).

[7] Surveillance capitalism describes a dominant economic model in which technology companies collect extensive personal user data (often passively and without full user comprehension) as a "behavioral surplus." This surplus is then analyzed, often using AI, to predict user behavior and is ultimately sold to advertisers and other third parties who wish to influence that behavior.

by Meta (formerly Facebook), is "surveillance-centered"[8] and relies on processing extensive off-site user data on proprietary servers to "expand ad audiences."[9] The financial incentive for this model is powerful; a large-scale study from the University of Chicago found that without this off-site data, the median cost per incremental customer for advertisers rose by 37%.[10] This creates a direct financial incentive against data minimization, as doing so would harm the core advertising revenue stream.

Meta's development of VR hardware constitutes a new, more powerful tool for this data-extraction model.[11] Meta XR functions as an "advertising platform"[12] designed for "data extraction"[13] on an unprecedented scale. Meta's own policies state that it processes "extensive and highly sensitive personal data,"[14] including biometric data from the Quest Browser and location data from IP addresses.[15] Meta's patents, End User Licence Agreements, and executive statements evidence corporate ambitions for sophisticated biometric tracking, including facial expressions and eye tracking,[16] to "further empower Facebook's advertising arm."[17]

In stark contrast, Apple's Vision Pro Headset is framed as "privacy-by-design"[18] in its technical documentation.[19] This architecture relies on two key principles: data minimization and on-device processing. Data minimization requires the company to collect only data "necessary to support seamless spatial experiences,"[20] while on-device processing dictates that maximum data be processed locally rather than on external servers.[21] This approach applies to the most sensitive data, including Optic ID (iris authentication), environmental mapping,[22] and hand tracking.[23]

The most sophisticated element of this design is the distinction between intent and raw gaze. Apple's system prevents developers—and Apple itself—from accessing a user's raw, continuous, subconscious eye-tracking data. Apps remain unaware that the user is looking at a "buy" button until the user performs a conscious selection gesture. This mechanism directly mitigates the risk of

---

[8] Ben Egliston & Marcus Carter, *Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse*, 10 INTERNET POL'Y REV. 8 (2021).

[9] *Toward Fairness in Personalized Ads*, META 8 (2023), https://about.fb.com/wp-content/uploads/2023/01/Toward_fairness_in_perso

[10] Nils Wernerfelt et al., *Estimating the Value of Offsite Data to Advertisers on Meta* § 6.3.1 (Becker Friedman Inst., Working Paper No. 2022-114, 2022).

[11] Egliston & Carter, *supra* note 8, at 3.

[12] *Id.* at 8.

[13] *Id.*

[14] Xynogalas & Leiser, *supra* note 4, at 93.

[15] *Id.*

[16] *Id.* at 96.

[17] Egliston & Carter, *supra* note 8, at 8.

[18] Privacy-by-Design (PbD) is an engineering approach where privacy and data protection are integrated into the design and architecture of IT systems, business practices, and services from the very beginning, rather than being added as an afterthought. This proactive framework ensures that personal data is automatically protected, making privacy the default setting for any system or product.

[19] *Apple Vision Pro Privacy Overview*, APPLE INC. 3 (2024).

[20] *Id.* at 4.

[21] *Id.* at 3.

[22] Environmental Mapping is the process by which an XR device uses its outward-facing cameras and sensors to scan the user's physical surroundings. This scan creates a real-time, 3D model of the room, including the position of walls, furniture, and other objects, allowing digital content to be realistically placed in, or interact with, the real-world space.

[23] *Apple Vision Pro Privacy Overview*, *supra* note 18, at 4.

"biometric psychography"[24] and subconscious thought inference.[25] While privacy-protective, this architecture also serves a competitive function. Because some of Apple's strict data restrictions do not apply to its own first-party apps, privacy becomes a mechanism for Apple to "get a head start in dominating the Vision Pro app market,"[26] highlighting tensions between privacy, competition, and corporate control.

III. THE NATURE OF IMMERSIVE HARM

Immersive technologies introduce novel forms of virtual violence, including embodied assaults and virtual rape. These "novel forms of gendered harm"[27] transcend textual or verbal abuse, involving virtual touching, grabbing, and groping of a user's avatar. The key factors amplifying this harm are embodiment—the sense that one's avatar is the same as one's physical body—and immersion. Because the harassment is felt as directly connected to the body, the psychological impact is not merely virtual. A British police investigation into a case of "virtual rape" concluded that the attack left the victim with the "same psychological and emotional trauma as someone who has been physically sexually assaulted."[28]

Beyond direct harm, a unique phenomenon of behavioral manipulation known as the "Proteus Effect" allows users to "infer their expected behaviors and attitudes from observing their avatar's appearance."[29] For example, users given taller avatars negotiate "more aggressively,"[30] and users with more attractive avatars perform better in online games.[31] Crucially, these behavioral changes transfer to the real world. A Stanford University study found that participants who embodied taller avatars in VR "would be more aggressive negotiators in a face-to-face interaction outside of the virtual environment than participants who had been in shorter avatars."[32]

This creates a vector for real-world manipulation. Studies indicate that participants in VR who saw their own avatar "self-endorse" a product reported "higher brand attitudes, purchase intention and brand preference."[33] A corporation utilizing a surveillance-based model could theoretically place a user in an avatar designed to leverage the Proteus Effect, rendering them more susceptible to advertising or political messaging, with behavioral effects persisting after the headset is removed.

---

[24]Biometric Psychography refers to the practice of building detailed psychological profiles of users based on their involuntary biological responses. In the context of XR, this involves inferring a user's subconscious interests, emotional state, or cognitive patterns from passively collected data like raw eye-gaze patterns.

[25]Richard Koch, *What Are You Looking At? Emerging Privacy Concerns with Eye Tracking in Virtual Reality*, 21 COLO. TECH. L.J. 1, 1-6 (2023).

[26]Mariana Olaizola Rosenblat, *Apple's Data Access Limits on Its Vision Pro Are Good for Privacy - and Also Good for Its Business*, NYU STERN CTR. FOR BUS. & HUM. RTS. (Oct. 27, 2025), https://bhr.stern.nyu.edu/quick-take/apples-data-access-limits-on-its-vision-pro-are-good-for-privacy-and-also-good-for-its-business/.

[27]Clare McGlynn & Carlotta Rigotti, *From Virtual Rape to Meta-Rape: Sexual Violence, Criminal Law and the Metaverse*, 45 OXFORD J. LEGAL STUD. 554, 554 (2025).

[28]*Id.* at 555.

[29]Nick Yee et al., *The Proteus Effect: Implications of Transformed Digital Self-Representation on Online and Offline Behavior*, 36 COMM. RSCH. 285, 287 (2009).

[30]*Id.* at 296.

[31]*Id.* at 306.

[32]*Id.* at 308.

[33]Rabindra Ratan et al., *Avatar Characteristics Induce Users' Behavioral Conformity with Small-To-Medium Effect Sizes: A Meta-Analysis of the Proteus Effect*, 22 MEDIA PSYCH. 651, 654 (2019).

IV. THE OBSOLESCENCE OF EXISTING LAW

The traditional legal foundation for data privacy in the West is the "notice and choice" model,[34] which relies on users giving "informed consent" via text-based privacy policies.[35] This model is futile in the context of virtual reality. First, the data collection is subconscious; the technology captures "eye motion and expressions"[36] and "hand and finger movements."[37] A user cannot logically consent to disclosing data they are unaware they are producing. Second, this leads to a "knowledge shift"[38] where companies "may know the user better than the user knows themselves,"[39] undermining the premise of informed consent.

Even robust data privacy frameworks like the GDPR are challenged by inferred data,[40] or information created by a system through analysis rather than explicit collection. A user's concentration level is not biometric data per se, but an inference derived from it, placing it in a legal grey area. The U.S. legal landscape remains a "patchwork"[41] of state-level laws, such as the Illinois Biometric Information Privacy Act (BIPA).[42] These laws center "around data collected or recorded for identification or authentication purposes."[43] This focus on identification creates a significant loophole, failing to regulate data collected for inference and profiling—the very data XR systems are designed to capture.

V. THE SEARCH FOR A NEW GOVERNANCE MODEL

In response to this regulatory failure, calls have intensified for "comprehensive national privacy legislation,"[44] such as a "Biometrics and an AI Bill of Rights."[45] Such legislation would mandate the technical architecture of privacy-by-design, transforming Apple's voluntary model into a public requirement. Policy blueprints have called for mandating data minimization,[46] effectively codifying corporate best practices into law.

A more novel solution proposed by the IEEE Global Initiative on Ethics of Extended Reality is

[34]The "notice and choice" model is a foundational data privacy framework where organizations (1) provide "notice" to individuals detailing how their personal information will be collected, used, and shared, and (2) offer a "choice" (such as an opt-in or opt-out) for the individual to consent to or reject those practices.

[35]Yeji Kim, *Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent*, 110 CALIF. L. REV. 225, 256 (2022).

[36]Dick, *supra* note 5, at 8.

[37]*Id.* at 7.

[38]Kim, *supra* note 34, at 226.

[39]*Id.* at 256.

[40]*Id.* at 228.

[41]Dick, *supra* note 5, at 18.

[42]Dan Carlston, *Biometric Privacy Law as Applied to Virtual Reality and Immersive Technologies*, COLUM. SCI. & TECH. L. REV. BLOG (Jan. 31, 2022), https://journals.library.columbia.edu/index.php/stlr/blog/view/420. BIPA grants a "private right of action," allowing individual citizens to sue companies for improper collection of biometric data.

[43]*Id.*

[44]Dick, *supra* note 5, at 22.

[45]Margaret Hu, *Biometrics and an AI Bill of Rights*, WM. & MARY L. SCH. SCHOLARSHIP REPOSITORY 301 (2022).

[46]Giovanni Sorrentino & Javier López-Guzmán, *Rethinking Privacy for Avatars: Biometric and Inferred Data in the Metaverse*, 6 FRONTIERS IN VIRTUAL REALITY 9 (2025).

the "Bodyright" framework.[47] Modeled on copyright law, this framework would grant individuals an "economic right" and a "moral right" to control how others use their biometric identity and "virtual clones."[48] This concept reframes data privacy as a property and human right, rendering one's biometric data an inalienable part of their identity with legal protections analogous to copyright.

VI. CONCLUSION

Immersive technology creates significant new biometric and psychological risks by enabling access to a user's subconscious data. This paradigm shift exposes a governance gap where existing laws are rendered obsolete. While the industry offers voluntary, technical solutions like Apple's "privacy-by-design," and scholars propose mandatory legal solutions like the IEEE's "Bodyright," reliance on the former is insufficient. Economic theory dictates that privacy is a public good; "an individual who is careless with data exposes not only extensive information about herself, but about others as well."[49] Voluntary solutions cannot solve such public good problems. Furthermore, the economic incentives for surveillance—quantified by the 37% rise in advertiser costs without offsite data—are too substantial to rely on corporate goodwill.[50] Therefore, a robust public legal framework is required to mitigate the embodied harms of inferred data.

[47] Thommy Eriksson, *Industry Connections Report: The IEEE Global Initiative on Ethics of Extended Reality (XR) Report*, IEEE 16 (Nov. 2021).

[48] *Id.*

[49] Joshua Fairfield et al., *Privacy as a Public Good*, 65 DUKE L.J. 385, 385 (2015).

[50] Wernerfelt et al., *supra* note 10, § 6.3.1.