Sean Balbale

Professor Brittany Starr

RHET 125

November 6, 2025

Embodied Harms and Inferred Data: Redefining Privacy in Virtual Reality

Introduction

The emergence of Extended Reality[1] (XR), an umbrella term for Virtual and Augmented Reality (VR/AR) technologies, represents a massive shift in human-computer interaction. Unlike previous eras, where data collection is technically optional, immersive technologies require continuous collection of intimate user data to function correctly. This new data-gathering model creates ethical and technical challenges. The primary risk is not identification (e.g., iris or fingerprint scans), but inference. These systems passively collect "behavioural biometrics" subtle head motions, hand movements, and eye-gaze patterns (Dilshani Kumarapeli et al. sec. 1). The power of these new data streams is significant; technical analyses have demonstrated that VR users can be "uniquely recognised with approximately 90% accuracy using head motions" (sec. 2.1) alone. This data enables platforms to infer sensitive information that individuals did not choose to disclose, including mental and physical health status (sec. 2.2), sexual preferences (Dick 11), and concentration levels (Xynogalas and Leiser 91).

This fundamentally moves the locus of data collection from an active process (such as clicks or text entries) to a passive one. The research on this topic converges into four primary clusters: (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. Reviewing this literature reveals a

[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.

critical gap between voluntary, corporate-led technical solutions and the growing demand from legal scholars for legally mandated public frameworks.

Competing Architectures of Control

The literature reveals a central discrepancy in the field: two opposed corporate philosophies for managing this new data stream—server-side surveillance and on-device privacy. The surveillance capitalism model[2], which was pioneered by Meta (previously Facebook), is "surveillance-centered" (Egliston and Carter 8) and relies on processing extensive off-site user data on its own servers to "expand ad audiences" (Meta 8). The financial incentive for this model is powerful. One 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% (Wernerfelt et al., sec. 6.3.1). This creates a direct financial incentive against data minimization, since doing so would harm the core advertising revenue stream.

Therefore, Meta's development of VR hardware (through its 2014 acquisition of Oculus) has created a new, more powerful tool for the same data-extraction model (Egliston and Carter 3). The literature has characterized Meta XR as an "advertising platform" (8) designed for "data extraction" (8) on an unprecedented scale. Meta's own policies state that it processes "extensive and highly sensitive personal data" (Xynogalas and Leiser 93), including biometric data from the Quest Browser and location data from IP addresses (93). Meta's patents, End User Licence Agreements, and executive statements are clear evidence of corporate ambitions for more sophisticated biometric tracking, including facial expressions and eye tracking (96), to "further empower Facebook's advertising arm" (Egliston and Carter 8).

In stark contrast to the surveillance capitalism model, Apple's Vision Pro Headset is framed as "privacy-by-design"[3] in its white papers (Apple 3). This architecture is built on two key principles:

[2] 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.

[3] Privacy-by-Design (PbD) is an engineering approach where privacy and data protection are integrated into the

data minimization and on-device processing. Data minimization requires the company only to collect data "necessary to support seamless spatial experiences" (4). On-device processing dictates that as much data as possible should be processed locally on the device instead of being sent to external servers (3). According to Apple's documentation, this on-device approach applies to the most sensitive data, including Optic ID (iris authentication), environmental mapping[4], and hand tracking (4).

The most sophisticated element of this design is the distinction between intent and raw gaze. Apple's system is built to prevent developers (and Apple itself) from accessing a user's raw, continuous, subconscious eye-tracking data. Apps are never told that the user is looking at the buy button. Only after the user performs a conscious selection gesture (such as a tap) is their finalized intent sent to the app. This is a direct solution to the risk of "biometric psychography"[5] and subconscious thought inference (Koch 120). While this is good for privacy, it is also a good business move because some of Apple's strict data restrictions (specifically regarding the device's cameras) do not apply to its own apps (Rosenblat), thus becoming a mechanism for Apple to "get a head start in dominating the Vision Pro app market" (Rosenblat). This complicates Apple's narrative as a purely privacy-focused actor and highlights tensions among privacy, competition, and corporate control.

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.

[4] Environmental Mapping is the process by which an XR device (like the Apple Vision Pro) 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.

[5] Biometric Psychography refers to the practice of building detailed psychological profiles of users based on their involuntary biological responses (i.e., "biometrics"). In the context of XR, this would involve inferring a user's subconscious interests, emotional state, or cognitive patterns from passively collected data like raw eye-gaze patterns, rather than from their conscious actions or inputs.

The Nature of Immersive Harm

The literature identifies new forms of virtual violence, including embodied assaults and virtual rape. These are described as "novel forms of gendered harm" (McGlynn and Rigotti 554) that go beyond textual or verbal abuse and include virtual touching, grabbing, and groping of a user's avatar. The key factors that amplify this harm are the feeling of embodiment—the sense that one's avatar is the same as one's physical body—and immersion—the feeling of being there. Since the harassment is felt as being directly connected to their body, the psychological impact is not virtual. One report analyzing a British police investigation of a case of "virtual rape" concluded that the attack left the victim with "same psychological and emotional trauma as someone who has been physically sexually assaulted" (555). The immersive nature of the technology, combined with the potential for algorithmic bias, discrimination, and manipulation creates unique challenges to a user's psychological and emotional well-being.

Moving beyond direct harm, the literature analyzes a unique phenomenon of behavioural manipulation known as the "Proteus Effect". This is a phenomenon in which users "infer their expected behaviors and attitudes from observing their avatar's appearance" (Yee et al. 2). For example, studies found that users given taller avatars negotiate "more aggressively" (22). Users with more attractive avatars perform better in online games (21). The most significant finding, however, is that these behavioral changes transfer to the real world. One study on the Proteus Effect from Stanford University placed participants in immersive VR with either taller or shorter avatars. Not only did those with taller avatars negotiate more aggressively within the virtual environment, but they also "would be more aggressive negotiators in a face-to-face interaction outside of the virtual environment than participants who had been in shorter avatars" (22).

This creates a testable vector for real-world manipulation, such as a corporation placing a user in an avatar designed to make them more susceptible to advertising. It connects research on psychological harms directly back to research on business models. For example, one study found that participants in VR who saw their own avatar "self-endorse" a product reported "higher brand attitudes, purchase intention and brand preference" (Ratan et al. 654). A corporation utilizing a surveillance-based model could, theoretically, place a user in an avatar specifically designed to leverage the Proteus Effect, making them more susceptible to advertising or political messaging, with behavioral effects that persist long after they have removed the headset.

The Obsolescence of Existing Law

The traditional legal foundation for data privacy in the West is the "notice and choice" model[6], which relies on users giving "informed consent" (Kim 256) via text-based privacy policies. The legal literature is in strong agreement that this model is obsolete and futile in the context of virtual reality. This failure is rooted in two core problems. First, the data being collected is subconscious. The technology is designed to capture everything from "eye motion and expressions" (Dick 8) to "hand and finger movements" (Dick 7). A user cannot logically consent to giving away data that they did not consciously know they were producing. Second, this leads to a "knowledge shift" (Kim 226). Because XR technologies can identify, respond to, and shape a user's unconscious needs, they create a situation in which "companies may know the user better than the user knows themselves" (256), thereby undermining the central legal premise of informed consent.

Even the world's most robust data privacy laws are ill-equipped. The EU's GDPR, for example, is challenged by inferred data[7] (228). A user's concentration level is not itself biometric data but an inference derived from it, placed in a legal grey area. The US legal landscape is a "patchwork" (Dick 18) of state-level laws, such as Illinois's Biometric Information Privacy Act[8] (Carlston). These laws center "around data collected or recorded for identification or authentication purposes" (Carlston). This focus on identification creates a massive legal loophole, as it fails to regulate

[6] The "notice and choice" model is a foundational data privacy framework where organizations (1) provide "notice" to individuals (typically through a privacy policy) 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.

[7] Inferred data is information that is not explicitly collected from a user but is instead created by a system through analysis or combination of other data points.

[8] Often cited as the strongest state-level biometric privacy law in the U.S., BIPA is unique because it grants a "private right of action," allowing individual citizens (not just the attorney general) to sue companies for improper collection or handling of their biometric data, such as fingerprints, facial scans, or iris scans.

data collected for inference and profile—exactly the data that XR systems are designed to capture. Current laws are built on an obsolete paradigm (text-based consent for identification purposes) and are fundamentally incapable of governing the new paradigm (subconscious, inferred, embodied data).

The Search for a New Governance Model

In response to this "patchwork" (Dick 18), many policy-focused reports call for "comprehensive national privacy legislation" (22), such as a "Biometrics and an AI Bill of Rights" (Hu 301). This represents a legislative attempt to require all companies to adopt the technical architecture of the privacy-by-design model. Policy blueprints, including the White House's, have called for mandating data minimization (Sorrentino and López-Guzmán 9). This solution would take Apple's voluntary, corporate-led model and make it mandatory, public-led, and legally required for all market participants.

The most novel solution proposed comes from the IEEE Global Initiative on Ethics of Extended Reality. This group has proposed a new legal framework conceptualized as a "Bodyright" (Eriksson 16). Explicitly modeled on copyright law, this framework would grant individuals an "economic right" and a "moral right" to control how others may use their biometric identity and "virtual clones" (16). This concept seeks to reframe data privacy as a property and human right, where one's biometric data is an inalienable part of their identity, with legal protections analogous to the copyright one holds in their own creative work.

Conclusion

The literature reviewed in this paper shows that immersive technology creates significant new biometric and psychological risks by enabling access to a user's subconscious data. This new paradigm has created a governance gap, as existing laws are obsolete. In response, the research is actively debating new models, primarily falling into two camps: a voluntary, technical solution

(Apple's "privacy-by-design" model (Apple 3)) and a mandatory, legal solution (the IEEE's "Bodyright" concept (Eriksson 16)).

The critical gap in the research lies in the debate over whether a voluntary, corporate-led technical solution is sufficient. The research strongly suggests the answer is no. First, economic theory on public goods argues that privacy is a public good, not a private one; "An individual who is careless with data exposes not only extensive information about herself, but about others as well" (Fairfield et al. 385). Voluntary solutions are historically destined to fail in solving such public good problems. Second, the economic incentives for surveillance, as quantified by the 37% (Wernerfelt et al., sec. 6.3.1) rise in advertiser costs without offsite data, are simply too substantial to rely on corporate goodwill.

Works Cited

Apple. *Apple Vision Pro Privacy Overview: Learn How Apple Vision Pro and VisionOS Protect Your Data.* 2024, www.apple.com/privacy/docs/Apple_Vision_Pro_Privacy_Overview.pdf.

Carlston, Dan. "Biometric Privacy Law as Applied to Virtual Reality and Immersive Technologies." *Columbia.edu*, 31 Jan. 2022, journals.library.columbia.edu/index.php/stlr/blog/view/420. Accessed 2 Nov. 2025.

Dick, Ellysse. "Balancing User Privacy and Innovation in Augmented and Virtual Reality." *Itif.org*, Information Technology and Innovation Foundation | ITIF, 4 Mar. 2021, itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augm

Accessed 2 Nov. 2025.

Dilshani Kumarapeli, et al. "Privacy Threats of Behaviour Identity Detection in VR." *Frontiers in Virtual Reality*, vol. 5, Frontiers Media, Jan. 2024, https://doi.org/10.3389/frvir.2024.1197547. Accessed 2 Nov. 2025.

Egliston, Ben, and Marcus Carter. "Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse." *Internet Policy Review*, vol. 10, no. 4, Alexander von Humboldt Institute for Internet and Society, Dec. 2021, https://doi.org/10.14763/2021.4.1610. Accessed 2 Nov. 2025.

Eriksson, Thommy. *Industry Connections Report: The IEEE Global Initiative on Ethics of Extended Reality (XR) Report - Who Owns Our Second Lives: Virtual Clones and the Right to Your Identity.* Nov. 2021, standards.ieee.org/wp-content/uploads/import/governance/iccom/who-owns-our-second-lives-virtual-Clones-Ident

pdf.

Fairfield, Joshua, et al. "Privacy as a Public Good." *Duke Law Journal*, vol. 65, no. 3, 2015, scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3824&context=dlj.

Hu, Margaret. "Biometrics and an AI Bill of Rights." *William & Mary Law School Scholarship*

Repository, 2022, scholarship.law.wm.edu/facpubs/2078/. Accessed 2 Nov. 2025.

Kim, Yeji. "Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move beyond Text-Based Informed Consent." *California Law Review*, vol. 110, no. 1, 2022, p. 225, lawcat.berkeley.edu/record/1228030?v=pdf. Accessed 2 Nov. 2025.

Koch, Richard. "What Are You Looking At? Emerging Privacy Concerns with Eye Tracking in Virtual Reality." *Colorado Technology Law Journal*, vol. 21, pp. 1-6, scholar.law.colorado.edu/cgi/viewcontent.cgi?article=1024&context=ctlj. Accessed 2 Nov. 2025.

McGlynn, Clare, and Carlotta Rigotti. "From Virtual Rape to Meta-Rape: Sexual Violence, Criminal Law and the Metaverse." *Oxford Journal of Legal Studies*, vol. 45, no. 3, Oxford University Press (OUP), 2025, pp. 554-82, https://doi.org/10.1093/ojls/gqaf009. Accessed 2 Nov. 2025.

Meta. *Toward Fairness in Personalized Ads*. 2023, about.fb.com/wp-content/uploads/2023/01/Toward_fairness_in_personalized_ads.pdf.

Ratan, Rabindra, et al. "Avatar Characteristics Induce Users' Behavioral Conformity with Small-To-Medium Effect Sizes: A Meta-Analysis of the Proteus Effect." *Media Psychology*, 2019, https://doi.org/10.1080/15213269.2019.1623698. Accessed 2 Nov. 2025.

Rosenblat, Mariana Olaizola. "NYU Stern Center for Business & Human Rights: Apple's Data Access Limits on Its Vision Pro Are Good for Privacy - and Also Good for Its Business." *Nyu.edu*, 27 Oct. 2025, bhr.stern.nyu.edu/quick-take/apples-data-access-limits Accessed 2 Nov. 2025.

Sorrentino, Giovanni, and Javier López-Guzmán. "Rethinking Privacy for Avatars: Biometric and Inferred Data in the Metaverse." *Frontiers in Virtual Reality*, vol. 6, Frontiers Media, May 2025, https://doi.org/10.3389/frvir.2025.1520655. Accessed 2 Nov. 2025.

Team, Secure Privacy. "Your Face, Eyes, and Hands: The Biometric Gold Rush in Apple Vision Pro." *Secureprivacy.ai*, 2025, secureprivacy.ai/blog/biometric-privacy-apple- Accessed 2 Nov. 2025.

Wernerfelt, Nils, et al. *Estimating the Value of Offsite Data to Advertisers on Meta*. 2022, bfi.uchicago.edu/wp-content/uploads/2022/08/BFI_WP_2022-114.pdf.

Xynogalas, Vasilis, and M. R. Leiser. "The Metaverse: Searching for Compliance with the General Data Protection Regulation." *International Data Privacy Law*, vol. 14, no. 2, Oxford University Press, Apr. 2024, https://doi.org/10.1093/idpl/ipae004.

Yee, Nick, et al. "The Proteus Effect: Implications of Transformed Digital Self-Representation on Online and Offline Behavior." *Communication Research*, vol. 36, no. 2, Jan. 2009, pp. 285-312, https://doi.org/10.1177/0093650208330254.