9 User Perspectives on Law-Sensitive Design in the Metaverse – Balancing Design, Regulation, and Acceptance

Florian Franke[23], Runjie Xie[24], and Benedikt Morschheuser[24]

9.1 Motivation

In recent decades, technological progress has advanced rapidly, while legal regulation has lagged behind and often struggles to keep pace. To govern the digital space, the European Union has introduced several major frameworks, including the *General Data Protection Regulation (GDPR)*, the *Digital Services Act (DSA)*, the *Digital Markets Act (DMA)*, and most recently the *AI Act*. These laws are deliberately drafted to be technology-neutral, outlining broad principles without prescribing their application to specific cases (Dickhaut et al., 2024). While this ensures general applicability and flexibility, it leaves wide room for interpretation. As a result, organizations often settle for the bare minimum of compliance, neglecting meaningful protections of user privacy and personal rights.

One emerging example is the *'metaverse'*. With advances in virtual world and *Extended Reality (XR)* technologies, the metaverse is envisioned as connected immersive 3D virtual spaces that enable users to engage in a wide range of activities, including gaming, socializing, attending events, and professional collaboration (Jadamba & Kang, 2025). Users, embodied as avatars, can interact with both human-controlled and AI-powered avatars in realistic ways. Accessing the metaverse is often realized by using XR devices, such as virtual reality headsets, which enhance immersion and allow avatars to mirror physical body movements and gestures. This heightened realism, however, requires the processing of sensitive biometric data (Xie et al., 2024).

Despite its potential, the metaverse poses major privacy and safety concerns. *First*, users are often unaware of the continuous collection of extensive and novel data from XR devices. *Second*, consent models are typically copied from static 2D environments that are ill-suited for continuous, multimodal, and highly sensitive metaverse data streams. *Third*, while the core idea of the metaverse and XR technologies is to deceive human senses, the dynamic nature of such environments can be exploited to subtly deceive and influence user perceptions and decisions, undermining autonomy. *Fourth*, heightened immersion increases risks of harassment and personal space invasions, which are widespread in virtual environments often perceived as anonymous and normless.

Scholars warn that current regulations such as the GDPR are too lax, vague, and insufficient to address these challenges in the metaverse (Chen et al., 2022; Dwivedi et al., 2022; Smith et al., 2023). Regulatory institutions remain largely unprepared, often lacking the expertise to address the complexity of immersive 3D environments (Benrimoh et al., 2022; Dwivedi et al., 2023; Smith et al., 2023). As a result, regulation advances slowly. In the absence of concrete design guidelines for lawful implementation in the metaverse, platforms tend to settle for minimalist compliance – copying inadequate 2D solutions into 3D contexts or, often, even failing to meet existing laws.

To tackle these privacy challenges, research on lawful design patterns is crucial (Dickhaut et al., 2024), especially those tailored to immersive 3D environments. The absence of actionable design guidelines for such environments represents a critical research and policy gap. To fill this gap, we developed law-sensitive design patterns based on prior literature, platform best practices, and expert consultation, targeting the four major privacy and personal rights issues in the metaverse. These patterns provide concrete guidance for platforms to implement lawful user protections. We

[23] ConPolicy GmbH – Institut für Verbraucherpolitik
[24] Gamification Research Group, Lehrstuhl für Wirtschaftsinformatik, Otto-Friedrich-Universität Bamberg

evaluated them using video-based vignettes created on Roblox in a representative online survey with 1,296 respondents, capturing both general attitudes toward privacy challenges and evaluations of the patterns in terms of effectiveness, immersion, use intention, safety, trust, and satisfaction.

9.2 Public Attitudes toward Privacy Rights in the Metaverse

At the beginning of our survey, we assessed general attitudes toward privacy in the metaverse by examining the perceived importance of data privacy and personal rights protection, support for related regulation, and willingness to pay for business models that safeguard these rights. Protecting privacy entails costs for platforms. For data privacy, platforms may need alternative revenue sources instead of relying on user data for personalized advertising or profiling, while for personal rights, platforms may need technical safeguards and hiring moderators.

Our results indicate that respondents place a high value on privacy: 94% of respondents rated data protection as rather or very important, and 93% rated the protection of personal rights similarly. A majority also favors stricter regulation. 89% support enhanced protection of personal rights, and 72% advocate stronger data privacy rules in the metaverse.

Regarding willingness to pay, 43% would pay for stronger data privacy e.g., to avoid profiling or personalized ads, and 34% would pay for enhanced protection of personal rights. The median willingness to pay was €10 per month per category. These findings contribute to current debates on "Pay or Consent" business models and the appropriate level of compensation.

9.3 Transparency on Continuous, Extensive Data Collection

A core data privacy challenge in the metaverse is individuals' lack of awareness about the pervasive and ongoing data collection and processing (Xie et al., 2024). Much of this tracking is embedded in platform backends, subtle, and largely invisible to users (McStay, 2023; Dwivedi et al., 2022). Beyond avatar-mediated interactions on the platform (Dwivedi et al., 2023), XR devices capture highly sensitive information such as body movement and biometric data (Adams et al., 2018).

Although GDPR mandates transparency, platforms often provide only minimal, generic disclosures, offering little concrete insight into what, when, and how data is collected. Many applications fail to meet these requirements and ongoing transparency during use has received little attention. This lack of clarity makes it nearly impossible for users, especially vulnerable groups, to fully understand the extent of data collection. As a result, many underestimate how extensively XR devices can track their actions in the metaverse, increasing the risk of exploitation by platforms.

Figure 1: Privacy Dashboard

Figure 2: Decentralized Privacy Assistants

To address this issue, we developed and tested *two design patterns*: *First*, a privacy dashboard visualizing real-time data collection with icons, and, *second*, a recurring reminder of ongoing data collection. These were tested against a *control condition resembling a standard 2D cookie banner*.

All conditions were evaluated in a simulated metaverse clothing store, where the platform tracked sensitive movements and heart rate data to optimize layouts and personalize the experience.

Consistent with the literature, nearly half of respondents had never heard of this issue in the metaverse. After being informed, however, 77% considered this issue rather or very problematic. Evaluation of the design patterns showed that recurring reminders were the most effective, making respondents more aware of ongoing data collection and feel subjectively better informed.

9.4 Consent Management in Immersive 3D Environments

Another core privacy challenge in the metaverse is the inadequacy of current consent management. Existing privacy notices often lack clarity and fail to explain XR-specific data collection (Adams et al., 2018; Happa et al., 2021). Platforms typically rely on long, vague, legal jargon-filled text notices, obscuring key details and broader implications of data collection consents (Abraham et al., 2022). They also fail to take advantage of the 3D virtual environment to clearly convey the complex data practices. As a result, users struggle to provide truly informed consent. Moreover, traditional mechanisms like cookie banners are particularly ineffective in immersive 3D environments, where interactions are dynamic and data processing requirements change frequently. This highlights the need for dynamic, context-sensitive consent mechanisms tailored to the metaverse.

To address this, we developed and tested *two design patterns* featuring virtual privacy assistants that provide interactive explanations of the consent process via text, visualization, and voice. These assistants can also answer follow-up questions, fully leveraging the metaverse's multimodal capabilities to convey complex information. The *first* design follows a decentralized approach, where each unit in the metaverse (e.g., a store) provides its own assistant to manage consent. The *second* follows a centralized approach, with a single platform-wide assistant managing user privacy preferences across all units. In this model, users set preferences upon first entering the metaverse, similar to a *Personalized Information Management System (PIMS)*, enabling unified management of data-sharing choices. These patterns were tested against traditional cookie banners as *control condition* in a scenario involving two different units: a virtual smartphone shop with low-sensitive data collection and a virtual gym with high-sensitive data collection.

Regarding familiarity with uninformed consent, 58% of respondents were previously unaware of it. After being informed, however, 75% considered it rather or very problematic. In the user evaluation, surprisingly, neither design pattern outperformed the control group, likely reflecting the challenge of balancing sufficient information provision with users' cognitive load, requiring further research.

9.5 Social Bot Labeling

The metaverse enables immersive experiences that blur the boundaries between reality and virtuality, leaving users vulnerable to deceptions that manipulate human senses. Since avatars can be controlled by either human or AI, it is often not immediately apparent whether an interaction partner is a real person or an AI-driven entity (Falchuk et al, 2018). AI-powered avatars (also known as social bots) can be hyperrealistically animated (Abraham et al., 2022), engage in humanlike interactions (McStay, 2023), and impersonate real users, thereby functioning as social bots. As known from 2D online contexts, such bots can exert considerable influence on human decision-making, including product recommendations and political opinion formation. Yet, many AI-driven avatars in the metaverse remain unlabeled, making them difficult to be distinguished.

To address this, recent regulations mandate AI labeling, including Article 50 of the EU AI Act (effective August 2025) and §18(3) of the German Interstate Media Treaty. Both require AI to be labeled in a human-understandable way but without specifying concrete design standards.

We designed and tested three patterns. The first involved bot identity disclosure at first contact (e.g., "I am an AI bot."). The second applied a visual marker, outlining bot avatars with a colored border. The third introduced bot-free zones, guaranteeing areas without bots. Identity disclosure at first contact, already partially practiced on platforms like Decentraland, served as the control condition. The conditions were evaluated in a virtual shopping scenario, where certain bot avatars were present in the store to provide recommendations aimed at influencing users' purchasing behavior.

When assessing familiarity with this emerging issue, about half of the respondents had never heard of social bots. After being informed, however, 69% considered the issue rather or very problematic. User evaluation showed that bot identity disclosure at first contact was rated as the most effective design pattern, both objectively measured and subjectively reported by individuals, and was considered the most helpful for identifying bots.

Figure 3: Bot Identity at First Interaction

Figure 4: Harassment Scenario Design

9.6 Protection against Harassment and Personal Space Invasions

Harassment is a persistent problem in online social environments and the metaverse is no exception. Victims are often women, children, and minoritized users (Dwivedi et al., 2023). Unlike in 2D spaces, harassment and personal space invasions in immersive, avatar-mediated environments can feel more immediate and intense, amplifying psychological and emotional harm and spilling over into victims' offline lives (Freeman et al., 2022). In these settings, harassment goes beyond visual and verbal forms and also includes physical and sexual assaults, such as non-consensual touching or slapping. With haptic devices, these attacks can be physically perceived (McIntosh & Allen, 2024).

Although legislation such as the DSA (Art. 9–24) formally protects against personal rights violations, it generally only applies after harm has occurred. Furthermore, the global nature of virtual spaces, with users from diverse cultural and legal contexts, makes it difficult to establish universally accepted definitions of harassment and personal space invasion.

This underscores the importance of design patterns for technical safety features. We examined two design patterns: First, a proactive safety bubble, which forms an invisible zone around the avatar to protect it from unauthorized interactions by restricting visibility of unauthorized intruders, and, second, a blocking function, which renders disturbing avatars invisible and inaudible to affected users. These were tested against a control condition without any safety features, in which the user could only escape harassment by running away and logging out. The conditions were evaluated in a simulated socializing scenario in a virtual club.

Regarding familiarity with this issue, about two-thirds of respondents reported never having heard of it. After a brief explanation, 58% rated it as rather or very problematic. User evaluations indicated that the safety bubble was perceived as the most effective and satisfactory solution.

9.7 Conclusion

We highlight four key privacy challenges in the metaverse: opaque ongoing data collection, inadequate consent management, AI-driven social bots, and virtual harassment. Our findings show that individuals are largely unaware of these risks but consider them highly problematic once informed. A notable proportion of respondents are willing to pay for stronger protection. More research is needed on appropriate information and consent mechanisms for the metaverse. For bot labeling, we found that identity disclosure at first interaction is preferred, and safety bubbles appear most effective against virtual harassment. These results underscores the importance of proactive, user-centered design patterns that go beyond minimalist regulatory compliance, guiding developers, platform owners, and policymakers in creating a privacy-protecting metaverse.

Acknowledgements

The research project PRIME (www.privacy-metaverse.de) underlying this paper was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) under funding code 16KIS1894K. Responsibility for the content of this publication lies with the authors.

References

Abraham, M., Saeghe, P., McGill, M., & Khamis, M. (2022). Implications of XR on Privacy, Security and Behaviour: Insights from Experts. *Nordic Human-Computer Interaction Conference*, 1-12.

Adams, D., Bah, A., Barwulor, C., Musabay, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. *USENIX Symposium on Usable Privacy and Security*, Baltimore, MD, USA, 443-458.

Benrimoh, D., Chheda, F. D., & Margolese, H. C. (2022). The Best Predictor of the Future – the Metaverse, Mental Health, and Lessons Learned From Current Technologies. *JMIR Mental Health*, 9(10), e40410. https://doi.org/10.2196/40410

Chen, Z., Wu, J., Gan, W., & Qi, Z. (2022). Metaverse Security and Privacy: An Overview. *IEEE International Conference on Big Data*, Osaka, Japan, 2950-2959.

Dickhaut, E., Janson, A., Söllner, M., & Leimeister, J. M. (2024). Lawfulness by design – development and evaluation of lawful design patterns to consider legal requirements. *European Journal of Information Systems*, 33(4), 441-468. https://doi.org/10.1080/0960085X.2023.2174050

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542, 1-55.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*, 25, 2071-2114.

Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37(2), 52-61.

Freeman, G., Zamanifard, S., Maloney, D., & Acena, D. (2022). Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *ACM Hum. Comput. Interact.*, 6(CSCW1), 85.

Happa, J., Steed, A., & Glencross, M. (2021). Privacy-certification standards for extended-reality devices and services. *IEEE VRW*, Lisbon, Portugal, 397-398.

Jadamba, J. & Kang, D. (2025). There I was, being virtually groped: Explore psychological ownership and the framing of sexual harassment in the immersive virtual reality space. *Computers in Human Behavior*, 162, 108559, 1-10.

McIntosh, V., & Allen, C. (2024) What do policymakers need to know about harassment in the metaverse? *Front. Virtual Real.*, 5, 1-8.

McStay, A. (2023). The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy and Technology*, 36(13), 1-26.

Smith, C. H., Molka-Danielsen, J., Rasool, J., & Webb-Benjamin, J.-B. (2023). The World as an Interface: Exploring the Ethical Challenges of the Emerging Metaverse. HICSS.

Xie, R., Kirchner-Krath, J., & Morschheuser, B. (2024). Towards an Ethical Metaverse: A Systematic Literature Review on Privacy Challenges. *European Conference on Information Systems*, 6.