Embodied Privacy Consent as a Design Probe for Rethinking Privacy Decisions

VIKTORIJA PANEVA, LMU Munich, Germany

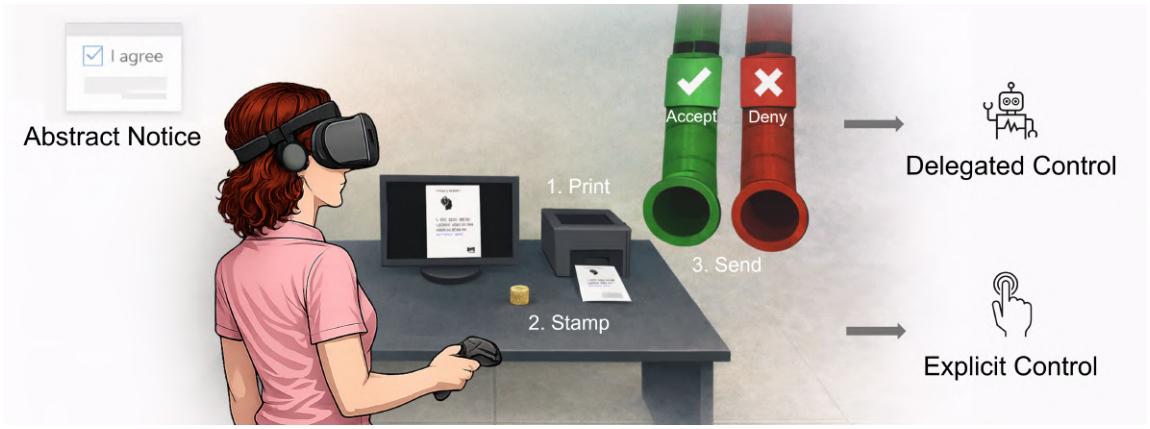

Fig. 1. In this position paper, we explore *embodied privacy consent* as a probe for examining the limits of individual decision-making, surfacing tensions between explicit, delegated, and hybrid control models for privacy permissions.

Consent mechanisms today predominantly rely on notice-and-choice approaches, placing the burden of privacy decision-making on the individual. These approaches are often front-loaded and detached from the moments when the data is required, leaving users to perform repetitive consent tasks with limited understanding of consequences. This position paper explores *embodied privacy consent* as a design probe to examine when, how, and whether active decision-making may be required. Drawing on an initial exploration of an embodied consent mechanism in Virtual Reality (VR), in which users enact consent through embodied action, we reflect on how such interactions make the act of consent experiential, allowing us to examine when active consent supports autonomy and when it becomes too burdensome or impractical. We argue that the embodied privacy consent probe can serve as a lens for surfacing tensions between explicit user control, delegated decision-making, and emerging hybrid models. We conclude by outlining potential consequences and future research directions for rethinking privacy decision-making in sensor-rich environments.

CCS Concepts: • **Human-centered computing** → **VR**; • **Security and privacy** → **Usability in security and privacy**.

Additional Key Words and Phrases: Usable Privacy, Privacy Consent, Virtual Reality (VR), Extended Reality (XR), Privacy Permissions, Embodiment, Interaction Design.

ACM Reference Format:

Viktorija Paneva. 2026. Embodied Privacy Consent as a Design Probe for Rethinking Privacy Decisions. In *Proceedings of Proceedings of the 2026 CHI Workshop on Moving Beyond Clicks: Rethinking Consent and User Control in the Age of AI (CHI '26).* ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

Author's Contact Information: Viktorija Paneva, viktorija.paneva@ifi.lmu.de, LMU Munich, Munich, Germany.

Manuscript submitted to ACM

1 Introduction

The most common approach to gathering consent for data collection in digital systems today remains notice-and-choice [12]. In practice, however, this model has been shown to be of poor usability: consent is often front-loaded, reduced to binary choices, and shaped by manipulative, deceptive patterns [6]. Important information is frequently buried in lengthy legal texts [7], leaving users with a limited understanding of the impact of their privacy decisions [9, 13]. Moreover, current consent mechanisms do not scale well, leading many users to give up managing data permissions for the growing number of apps, services, and devices [11].

These challenges become particularly pronounced in emerging immersive technologies. Head-mounted display (HMD)-based environments, such as Extended and Virtual Reality (XR/VR), enable immersive experiences through always-on sensors and increasingly fine-grained data collection, including body movement, eye tracking, telemetry, and spatial context. Such data can support inferences about users' well-being, literacy, vision impairments, and even cognitive or affective states [4], while movement data alone can be used to uniquely identify users [5]. At the same time, users often have limited awareness of the granularity of these sensing capabilities and the inferences that can be drawn from them [2]. As smart systems with continuous sensing become widespread, privacy decision-making is no longer limited to discrete moments of disclosure but becomes entangled with ongoing, contextual, embodied interaction [3, 8].

This shift motivates the need to rethink how consent and control should be designed and when active privacy decision-making remains feasible and meaningful. While we ground this paper in immersive environments, embodied consent may also serve as a probe in other sensor-rich contexts characterised by continuous behavioural data collection, such as wearables, smart homes, social robots, and diverse AI-driven sensing systems.

2 Embodied Privacy Consent as a Probe

We define *embodied privacy consent* as a consent interaction performed through embodied action in context, often situated at the moment when data collection becomes relevant within an experience. We propose the use of embodied privacy consent as a *design probe* to examine broader questions of consent and control in sensor-rich systems.

In recent work, Paneva et al. explored embodied consent mechanisms situated in VR [10]. One example is the *Privacy Post* interface (see Figure 1), in which the user prints the privacy notice, acknowledges it by stamping the virtual document and then exercises consent by submitting it through an in-world pneumatic tube. This approach draws from reflective interaction design, where moments of interruption or effort can encourage active deliberation. In this vein, Distler et al. introduced the concept of security-enhancing friction: deliberate moments of negative UX in security-critical situations intended to reduce risk-taking behaviour without compromising the overall UX [1].

As a probe, embodied privacy consent can help investigate several tensions that shape the current landscape of consent and control. First, it foregrounds the *contextual threshold of being informed*. When consent is enacted at the moment data becomes relevant, we can examine what information users actually need in situ to understand the stakes of disclosure. Second, while embodied consent mechanisms surface the *burden of repeated active decision-making*, they can also reveal moments of friction that may be valuable in *slowing down disclosure* when the stakes are high.

Research Directions and Consequences. Treating embodied privacy consent as a probe shifts the discussion from optimising consent interfaces for efficiency towards the broader question of when individual consent remains meaningful or sustainable. Future work could examine how embodied consent functions across different data sensitivities and interaction workflows, including when friction supports reflection versus when it becomes burdensome, and when delegation (e.g., to trusted agents or institutional safeguards) or distributed models of control may be required. More

broadly, embodied consent probes can help explore how different interaction modalities reshape what counts as consent or refusal when privacy decisions are enacted through ongoing interaction rather than discrete agreements. Future studies could deploy embodied consent probes to systematically vary timing, frequency, and data sensitivity to map thresholds at which explicit consent supports autonomy versus when delegation or default minimisation becomes preferable.

3 Conclusion

In this position paper, we introduced *embodied privacy consent* as a situated consent interaction enacted through embodied action, and argued for its value as a design probe for rethinking privacy decision-making. We suggest that making consent experiential and contextual can help surface the limits of notice-and-choice approaches that rely on routine, case-by-case user decisions. As immersive and AI-enabled systems increasingly rely on continuous behavioural sensing, such probes could support the exploration of alternative futures of consent and control, including delegated and hybrid models that move beyond front-loaded decision-making.

References

[1] Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. 2021. The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. In *Proceedings of the New Security Paradigms Workshop 2020* (Online, USA) *(NSPW '20)*. Association for Computing Machinery, New York, NY, USA, 45–58. doi:10.1145/3442167.3442173

[2] Hilda Hadan, Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 784, 24 pages. doi:10.1145/3613904.3642104

[3] Shady Mansour, Verena Winterhalter, Florian Alt, and Viktorija Paneva. 2026. A Multi-Layered Privacy Permission Framework for Extended Reality. In *Proceedings of the 2025 New Security Paradigms Workshop (NSPW '25)*. Association for Computing Machinery, New York, NY, USA, 50–65. doi:10.1145/3774761.3774916

[4] Vivek Nair, Gonzalo Munilla Garrido, Dawn Song, and James O'Brien. 2023. Exploring the privacy risks of adversarial VR game design. *Proceedings on Privacy Enhancing Technologies* (2023).

[5] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg, and Dawn Song. 2023. Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 895–910. https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification

[6] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376321

[7] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147. arXiv:https://doi.org/10.1080/1369118X.2018.1486870 doi:10.1080/1369118X.2018.1486870

[8] Viktorija Paneva, Marvin Strauss, Verena Winterhalter, Stefan Schneegass, and Florian Alt. 2024. Privacy in the Metaverse:. *IEEE Pervasive Computing* 23, 3 (2024), 73–78. doi:10.1109/MPRV.2024.3432953

[9] Viktorija Paneva, Verena Winterhalter, Franziska Augustinowski, and Florian Alt. 2025. User Understanding of Privacy Permissions in Mobile Augmented Reality: Perceptions and Misconceptions. *Proc. ACM Hum.-Comput. Interact.* 9, 5, Article MHCI037 (Sept. 2025), 17 pages. doi:10.1145/3743738

[10] Viktorija Paneva, Verena Winterhalter, Naga Sai Surya Vamsy Malladi, Marvin Strauss, Stefan Schneegass, and Florian Alt. 2025. Usable Privacy in Virtual Worlds: Design Implications for Data Collection Awareness and Control Interfaces in Virtual Reality. arXiv:2503.10915 [cs.HC] https://arxiv.org/abs/2503.10915

[11] Sarah Prange, Pascal Knierim, Gabriel Knoll, Felix Dietz, Alexander De Luca, and Florian Alt. 2024. I do (not) need that Feature! – Understanding Users' Awareness and Control of Privacy Permissions on Android Smartphones. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA. https://www.usenix.net/conference/soups2024/presentation/prange

[12] Robert H Sloan and Richard Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L.* 14 (2014), 370.

[13] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–24.

Viktorija Paneva is a postdoctoral researcher at LMU Munich, working on usable security and privacy in emerging technologies.