Beyond the Static Click: Implementing Dynamic Consent and Rule-Based Privacy in Immersive XR

GEORGE E. RAPTIS, Human Opsis, Greece
ELENI CHRYSOPOULOU, Human Opsis, Greece
CHRISTINA KATSINI, Human Opsis, Greece

ACM Reference Format:
George E. Raptis, Eleni Chrysopoulou, and Christina Katsini. 2018. Beyond the Static Click: Implementing Dynamic Consent and Rule-Based Privacy in Immersive XR. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX)*. ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Digital environments often push users into privacy decisions, with designs that frequently stack these choices against the user. In Extended Reality (XR), headsets use cameras and sensors to collect sensitive biometric data continuously. Traditional "notice-and-consent" mechanisms, which rely on simple clicks, fail in these high-frequency data environments. Users cannot effectively manage their privacy when a device captures their facial expressions and eye movements every second.

The PRINIA project [1] addresses this by offering a privacy-preserving facial recognition module for XR. We move beyond static, one-time consent by implementing dynamic control mechanisms. Our approach enables users to manage their privacy settings in real time within immersive environments. This system translates complex legal requirements into actionable rules that protect user identity without stopping the functionality of the XR application. PRINIA protects users through the PEEP (Privacy using EigEnface Perturbation) model. This method adds noise to facial data before sending it to a server. This safeguard ensures that even if an attacker steals the stored data, they cannot reconstruct the user's original biometric identity. Our research shows that users value this protection; once informed about these safeguards, user preference for privacy-enhanced methods increased by 140%.

PRINIA addresses the workshop's key questions on "designing new mechanisms" and "understanding context". The project explores how emerging XR modalities reshape consent by replacing "clicks" with continuous, rule-based protection. Our user studies reveal that the context of a decision varies depending on the organization involved. We found that users trust public entities more than private companies, which reduces their perceived need for high levels of privacy noise. By providing a "privacy-performance slider," PRINIA offers a design provocation that empowers users to choose their own balance between system speed and data protection. This approach challenges current assumptions about individual responsibility and envisions a future in which AI-driven safeguards preserve user autonomy.

Authors' Contact Information: George E. Raptis, graptis@humanopsis.com, Human Opsis, Patras, Greece; Eleni Chrysopoulou, echrysopoulou@humanopsis.com, Human Opsis, Patras, Greece; Christina Katsini, ckatsini@humanopsis.com, Human Opsis, Patras, Greece.

Manuscript submitted to ACM

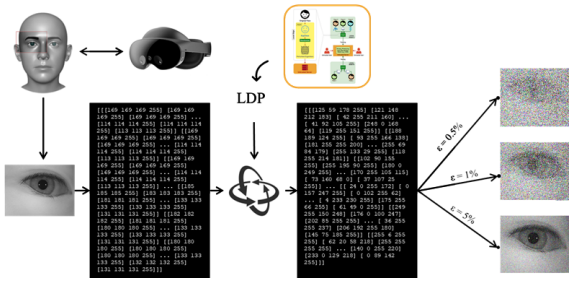

Fig. 1. Applying differential privacy enhancements in iris identification through PRINIA models.

2 PRINIA approach

2.1 Designing new safeguards

PRINIA (Fig. 1) implements a technical safeguard to protect biometric identity in XR environments. This model uses Local Differential Privacy (LDP) by adding Laplacian noise to the Eigenfaces extracted from raw facial data. By perturbing the data directly on the headset before it reaches any external server, the system ensures that unauthorized parties cannot reconstruct the original biometric templates. This approach minimizes data-transfer risks while maintaining high classification accuracy in facial recognition tasks. Beyond noise, PRINIA uses a rule-based framework that translates complex EU regulations (e.g., GDPR) into actionable privacy rules within the immersive scene. This system replaces static consent clicks with dynamic, real-time control. Users interact with a privacy-performance slider to adjust the privacy budget (epsilon) to their specific needs. A smaller epsilon provides stronger privacy by increasing noise intensity, though it may reduce system accuracy. This mechanism empowers users to manage their sensitive facial and eye-tracking data actively during the interaction.

2.2 Understanding context

We conducted a user study with 78 participants to understand the context of privacy decisions in high-stakes environments. We used a simulated airport where participants verified their identity at check-in and security checkpoints using facial recognition. The study compared a private airline and a public entity to measure how authority influences trust. Results showed a significant shift in user behavior when participants understood the privacy safeguards. Initially, 68% of participants preferred raw data for its speed. However, after learning that the PRINIA model protects their identity, preference for privacy-enhanced noise increased by 140%. Users demonstrated a high willingness to accept performance trade-offs, such as ticket processing delays of up to 15 minutes, to ensure their biometric data remained secure. The study also revealed that context significantly impacts the perceived need for safeguards. Participants trusted public organizations more than private companies to follow regulations and protect sensitive data. Consequently, users selected noise levels closer to the raw data when interacting with public authorities, indicating reduced reliance on high-intensity privacy noise in those contexts. These findings suggest that the threshold for being informed is not static but varies with the perceived accountability of the data controller.

2.3 Design provocation: The privacy - performance slider

PRINIA introduces a “privacy-performance slider” that allows users to control their data noise level directly. This tool adjusts the epsilon parameter, which controls the intensity of Laplacian noise applied to facial characteristics. Higher

noise levels provide stronger privacy but increase processing time and reduce system accuracy. Our study reveals that participants do not always prioritize convenience; when given a choice, most individuals selected a moderate-to-high privacy setting, represented by level 11 on our experimental scale. This finding serves as a design provocation against the current industry focus on seamless, instant interactions. Many participants willingly accepted ticket processing delays of up to 15 minutes to ensure the system did not store their raw biometric identity. This behavior suggests that users value data sovereignty over immediate gratification in high-stakes environments like airports. The slider transforms the user from a passive data subject into an active negotiator of their privacy budget. It challenges designers to offer meaningful trade-offs instead of "optimized" settings that prioritize corporate data collection over user comfort.

3 Implications and future outlook

The adoption of PRINIA leads to implications and consequences for user autonomy and agency in AI-driven environments. Our results show that 54.8% of users prefer biometrics only when the system includes privacy protections. This approach addresses the “broken” notice-and-consent landscape by moving individual responsibility to automated, yet user-defined, safeguards. By using a rule-based system that adheres to regulations (e.g., GDPR), the framework reduces the cognitive burden of managing continuous data streams in XR headsets. PRINIA differs from prior work by combining local differential privacy with empirical insights into user trust and authority. While previous systems often forced a binary choice between “on" and “off," PRINIA provides a spectrum of control that preserves agency. The anticipated consequence is a shift toward "biometrics with privacy" as the new standard for immersive authentication. This evolution ensures that users remain in control of their sensitive ocular and facial data without needing to perform a manual “click" for every second of sensor capture. Future research should explore how these distributed control models can scale across different public and private sectors to maintain a consistent threshold for being informed.

Authors’ biographies

Dr. George E. Raptis (MEng, MSc, PhD; https://raptisg.com) is a System Architect at Human Opsis. His expertise includes system architecture, DevSecOps, and risk assessment. His current research focus is on building resilient distributed systems that protect user data in immersive environments.

Eleni Chrysopoulou (BSc) is a researcher at Human Opsis, specializing in XR, human–computer interaction, and secure-by-design digital systems. Her work focuses on immersive XR applications in healthcare and biometric authentication, contributing to the development and validation of innovative platforms.

Christina Katsini (MEng, MSc, PhDc; http://katsinic.com) is a Usable Security and Privacy Lead at Human Opsis. Her expertise includes human-centered security evaluation, UX-driven audits, and privacy-by-design principles. She is interested in creating adaptive user interfaces that allow individuals to manage their data effectively in XR.

Acknowledgments

This work was partially supported by the European Union’s Horizon Europe Research and Innovation Programme under the CONSOLE project (Grant Agreement No. 101128070)

References

[1] George E. Raptis, Christina Katsini, Nicholas Hadjisavvas, and Efstathios Stavrakis. 2024. PRINIA: Privacy-Preserving Facial Recognition Framework for Extended Reality Environments. In *2024 International Conference on Computer and Applications (ICCA)*. IEEE, 1–6. doi:10.1109/icca62237.2024.10928041