frontiers in Virtual Reality

TYPE Original Research
PUBLISHED 07 May 2026
DOI 10.3389/frvir.2026.1779260



OPEN ACCESS

EDITED BY
Albert Rizzo,
University of Southern California,
United States

REVIEWED BY
Helmut Schrom-Feiertag,
Austrian Institute of Technology (AIT),
Austria
Mariachiara Tirinzoni,
Independent Researcher, Milan, Italy

*CORRESPONDENCE
Giuseppe Alessandro Veltri,
giuseppe.veltri@unitn.it

RECEIVED 01 January 2026
REVISED 12 April 2026
ACCEPTED 13 April 2026
PUBLISHED 07 May 2026

CITATION
Veltri GA, Mureddu F, Innocenti A, Sirizzotti M and Venturini E (2026) Regulatory frameworks and digital identity in the metaverse: an exploratory virtual reality experiment on trust, privacy, and openness.
*Front. Virtual Real.* 7:1779260.
doi: 10.3389/frvir.2026.1779260



# Regulatory frameworks and digital identity in the metaverse: an exploratory virtual reality experiment on trust, privacy, and openness

Giuseppe Alessandro Veltri[1,2]*, Francesco Mureddu[3], Alessandro Innocenti[4], Matteo Sirizzotti[5] and Eva Venturini[4]

[1]Department of Sociology and Social Research, University of Trento, Trento, Italy, [2]Centre for Behavioural and Implementation Science Interventions (BISI), Yong Loo Lin School of Medicine, National University of Singapore, Singapore, Singapore, [3]The Lisbon Council for Competitiveness and Social Renewal, Department of Design, Politecnico di Milano, Milan, Italy, [4]LabVR UNISI, Department of Social, Political and Cognitive Sciences, University of Siena, Siena, Italy, [5]Dipartimento di Architettura e Disegno Industriale, Università degli Studi della Campania "Luigi Vanvitelli", Caserta, Italy

**Introduction:** The rapid expansion of immersive metaverse platforms raises pressing questions about how governance and digital identity should be designed to foster trust, protect privacy, and support inclusive participation. Empirical evidence on how different governance and identity regimes are experienced *in situ* through virtual reality interfaces remains limited.
**Methods:** We conducted an exploratory VR experiment with 101 participants using a 2 × 2 design. The study contrasted two stylised governance configurations—a council-regulated metaverse and a comparatively unregulated "wild-west" environment—and two identity conditions: identity-disclosure cues versus anonymous interaction. Outcomes included perceived trust and privacy, openness to sustainability-related content, spatial presence, and simulator sickness.
**Results:** Council-regulated environments significantly increased perceived trust and privacy and substantially reduced simulator sickness compared to wild-west conditions. Identity-disclosure cues did not affect trust or openness but were associated with higher spatial presence. Correlational analyses further indicated that trust and privacy perceptions were strongly linked to openness and comfort in VR.
**Discussion:** The findings suggest that governance cues experienced within immersive environments can meaningfully shape user experience, and that proportionate, context-sensitive identity arrangements may be preferable to blanket real-name policies. These results inform ongoing debates on the design of open, human-centric virtual worlds and provide empirical insights relevant for platform governance and policy development.

KEYWORDS
digital identity, governance, metaverse, presence, privacy, regulation, trust

## 1 Introduction

The rapid emergence of immersive "metaverse" platforms has renewed longstanding debates on how identity, privacy and governance should be organised in networked environments. Beyond entertainment, extended-reality (XR) technologies are increasingly envisioned as infrastructures for education, work, public services and civic participation. In Europe, this evolution is explicitly framed by a policy ambition to foster

open, human-centric virtual worlds that are interoperable, inclusive, ethically and environmentally responsible, and that strengthen the technological sovereignty of European industry. The Horizon Europe coordination and support action OPENVERSE (Open and co-created Virtual Worlds for Europe) responds to this agenda by building a shared knowledge base on virtual worlds, animating a multi-stakeholder community, exploring ethical, legal, IPR and single-market challenges, and co-developing a technology and policy roadmap for open virtual worlds in Europe. Within this broader vision, questions of digital identity and regulation are strategically central. Virtual worlds depend on fine-grained behavioral telemetry, biometric indicators and cross-context identifiers, making them fertile ground both for innovative identity solutions and for new forms of surveillance and profiling. At the same time, the European regulatory "stack" – from the (General Data Protection Regulation) GDPR to the Digital Services Act, Digital Markets Act, AI Act and eIDAS 2.0 (Electronic Identification, Authentication and Trust Services) – is beginning to define concrete obligations for platform governance, risk mitigation and high-assurance digital identity across borders. How identity is represented (pseudonymous versus verified), how data flows are constrained, and how governance responsibilities are distributed between private platforms, public authorities and hybrid arrangements are not merely technical design parameters; they shape users' felt sense of safety, dignity, agency and inclusion in immersive environments. Existing scholarship has mapped many of these tensions conceptually, highlighting the trade-offs between anonymity and accountability, the risks of XR-specific biometrics and inference, and the promise of privacy-preserving identity architectures based on decentralised identifiers and verifiable credentials. However, there is still limited empirical evidence on how concrete governance framings and identity policies in metaverse platforms affect users' lived experience–for example, their trust in the environment, their willingness to disclose or engage with sensitive content, their sense of presence and their physical comfort. In particular, little is known about how users respond to different combinations of regulatory cues (e.g., "institutionally regulated" versus "wild-west" platforms) and identity regimes (identity-disclosure cues versus pseudonymous or anonymous participation) when these are encountered *in situ* through XR interfaces rather than as abstract policy descriptions. This paper contributes to filling that gap by reporting an exploratory virtual-reality experiment conducted in the framework of OPENVERSE, and specifically aligned with its work on barriers and policy gaps for governance and business models in virtual worlds. Using commercially available VR platforms as testbeds, we implemented a 2 × 2 design contrasting two stylised governance configurations (a "council-regulated" versus a "wild-west" metaverse) and two identity conditions (identity-disclosure cues versus anonymous interaction). We then examined how these configurations influenced participants' perceptions of trust and privacy, their openness to sustainability-oriented content, their sense of presence and their levels of simulator sickness. The aim is twofold: empirically, to characterise the experiential effects of different metaverse governance and identity regimes; and strategically, to inform the OPENVERSE roadmap and related European discussions on how to operationalise "open and human-centric" virtual worlds in ways that are both rights-respecting and practically workable.

The metaverse is best understood as a constellation of immersive, persistent and socially networked environments that blend spatial computing with real-time interaction, where identity is enacted through embodiment, gesture, voice and behavioral telemetry rather than mainly through text or static profile fields, which intensifies longstanding tensions around **privacy, safety and governance**. Classic internet research showed that networked spaces invite experimentation and multiplicity of selves (Turkle, 1995), while ethnographies of virtual worlds such as Second Life documented how communities build norms, jurisdictions and sanctioning practices that are always shaped by platform affordances (Boellstorff, 2008). In immersive media these dynamics are amplified because social presence - the felt sense of "being with" others - is heightened by multimodal cues and low-latency feedback (Short et al., 1976; Biocca and Harms, 2002; Son et al., 2025). As a result, apparently technical choices about how **identity is represented** (pseudonymous versus verified), how data flows are organised (granularity and retention of telemetry) and how governance is implemented (platform-centric versus public or shared oversight) are experienced directly by users as questions of dignity, safety and agency. Work on **presence and co-presence** shows that immersion and interaction quality are tightly linked to the sense of "being there" together (Schubert et al., 2001; Witmer and Singer, 1998; Tran et al., 2024), and recent social VR studies indicate that interface design, moderation tools and community norms can significantly modulate perceived social presence, trust and willingness to interact (Son et al., 2025; Jin, 2024). This makes identity design inseparable from governance design: the way users appear, authenticate and signal their roles is directly tied to how safe and accountable a metaverse environment feels. **Identity itself is not neutral**. Research on avatars and the **Proteus effect** shows that avatar characteristics can influence both user behavior and how others respond to them (Yee and Bailenson, 2007; Yee et al., 2009), and meta-analytic work points to small-to-moderate behavioral conformity effects that are sensitive to context and design (Ratan et al., 2020; Coesel, 2024). In the metaverse, where representation is often full-body, persistent and used across activities, design choices about whether to privilege stylised, fantastical avatars or more "realistic" ones interact with social norms, self-expression and moderation capacity. Stylisation can support experimentation, play and minority self-expression; more realistic representations can aid accountability and reduce some forms of impersonation, but may also import offline biases, increase the salience of discrimination and make users more vulnerable to doxxing or cross-platform profiling (Yang et al., 2024). Debates over **pseudonymity and real-name policies** therefore reappear in a new guise: pseudonymity tends to support creativity and protection for stigmatised identities but can enable harassment and fraud if not combined with effective governance, whereas strong, public real-name regimes can chill speech and expose people to offline risks. The literature increasingly points towards **hybrid identity arrangements**, where pseudonymous "front-stage" identities are combined with context-specific "back-stage" verification for payments, age-gating or serious misconduct investigations, and where verification relies on selective-disclosure credentials and zero-knowledge proofs that allow users to prove attributes (for example, being over 18 or holding a particular professional role) without revealing their full civil identity (W3C, 2022; W3C, 2023; European Parliament and Council, 2024b).

In parallel, privacy theory has moved from Westin's (1967) early focus on individual control over personal information towards frameworks such as Nissenbaum's (2010) **contextual integrity**, which understands privacy as appropriate information flows relative to context-specific roles, norms and purposes. This lens is especially useful for XR, where the same gaze vectors or motion traces can be used for rendering, accessibility features, safety analytics, profiling or targeted advertising, and where the acceptability of each use depends on the situational context and legitimate expectations of the people involved. Empirical work on the **privacy calculus** suggests that users weigh perceived benefits of disclosure - personalisation, convenience, safety - against anticipated risks such as surveillance, harassment or data breaches (Dinev and Hart, 2006). In metaverse settings, this calculus is reshaped by embodiment and social presence: transparency, meaningful options and clearly communicated governance arrangements can increase willingness to share data, whereas opaque cross-context reuse and unclear accountability dampen participation, particularly among vulnerable or minoritised groups (Yang et al., 2024; Jin, 2024; Giaretta, 2025). **Communication Privacy Management (CPM) theory** conceptualises privacy as the ongoing coordination of boundaries within relationships, emphasising that once information is shared it becomes co-owned and requires explicit rules to prevent "boundary turbulence" when expectations diverge (Petronio, 2002). In immersive environments this translates into interface-level commitments about what is recorded, who can replay or access raw motion and voice data, and how conflicts are handled, with legible and easily accessible controls helping users to understand and manage those boundaries. These identity and privacy questions are sharpened by the deep **datafication of XR**. Under the GDPR, biometric data are defined as data resulting from technical processing of physical, physiological or behavioral characteristics that allow or confirm unique identification, and a growing body of work shows that head-and-hand trajectories, gait and gaze patterns can function as powerful **behavioural biometrics** (Pfeuffer et al., 2019; Miller et al., 2020; Nair et al., 2023; Rubo et al., 2025). Even relatively short segments of motion can be used to re-identify users across sessions and applications with high accuracy, so telemetry compromise can have longer-lasting consequences than password leaks and may be difficult or impossible to "reset". Security and privacy surveys in VR underline that the same data streams also allow inferences about cognitive state, affect or health-related characteristics (Giaretta, 2025), raising sensitivity even in the absence of explicit identification. From a contextual-integrity perspective, this makes **purpose limitation and proportionality** central: telemetry should be scoped to what is necessary, processed on-device whenever possible, minimised in granularity and retention, and shielded by strong technical and organisational safeguards, including differential access controls, time-bound storage and systematic Data Protection Impact Assessments (European Parliament and Council, 2016; Giaretta, 2025).

In the European context, these technical and design questions sit within an evolving **EU regulatory stack** that reaches well beyond the GDPR. The **Digital Services Act (DSA)** introduces due-diligence obligations and systemic risk-mitigation duties for online platforms, especially Very Large Online Platforms; metaverse providers falling under the DSA must identify and mitigate risks such as harassment, illegal content, disinformation and harms to vulnerable users, and identity policies (for example, around age assurance, bot detection and fraud prevention) are key levers but must themselves respect principles of transparency, necessity and non-discrimination (European Parliament and Council, 2022b; Jin, 2024; Hulkó et al., 2025). The **Digital Markets Act (DMA)** further constrains gatekeeper platforms' ability to combine personal data across services without consent, prohibits self-preferencing and strengthens interoperability, which matters in metaverse ecosystems where one company may control hardware, operating system, app store, identity and payments (European Parliament and Council, 2022a; Hulkó et al., 2025). The **AI Act** introduces a risk-based regime for AI systems, including those used for content moderation, recommendation, personalisation and behavioral analytics in immersive spaces, while imposing specific restrictions on biometric identification and emotion recognition; metaverse operators must map their AI-enabled safety and analytics tools to the appropriate risk categories and avoid prohibited practices (European Parliament and Council, 2024a; Yang et al., 2024). **eIDAS 2.0 and the European Digital Identity Wallet (EUDI)** create a complementary layer by defining cross-border, high-assurance identity and attribute credentials that can be selectively disclosed through verifiable credentials (European Parliament and Council, 2024b; W3C, 2022; W3C, 2023). In metaverse contexts, EUDI-compatible wallets could enable age-gated or role-restricted spaces, professional and educational environments and public-service interactions with strong assurance but minimal data transfer, supporting GDPR principles of data minimisation and purpose limitation while enhancing trust and legal certainty for cross-border participation. These core instruments are complemented by NIS2 for cybersecurity governance, consumer and product-safety law for XR devices, and emerging age-appropriate design and accessibility frameworks, all contributing to a layered notion of **"trustworthiness"** in which identity, security, usability and fairness are tightly coupled (European Parliament and Council, 2016; Hulkó et al., 2025; Giaretta, 2025). Translating this regulatory vision into concrete systems, much of the technical literature converges on **decentralised identifiers (DIDs)** and **verifiable credentials (VCs)** as a backbone for privacy-preserving, interoperable identity across XR experiences (W3C, 2022; W3C, 2023; Yang et al., 2024). In these architectures, users control **wallets** holding credentials issued by trusted entities such as public authorities, universities, employers or platforms, while verifiers request only the attributes needed for a given purpose and rely on selective disclosure and zero-knowledge techniques to avoid over-exposure of personal data. Credential presentation can occur locally on the user's device, with minimal metadata leakage, and trust frameworks with defined assurance levels and liability rules specify who may issue which credentials under what conditions, potentially linked to EUDI trust lists. However, research emphasises that **usability and legibility** are crucial: users must understand which attributes they are presenting, to whom and for what reason, and they need simple ways to revoke credentials, adjust consent and review their history of presentations, otherwise technically sophisticated solutions may still fail in practice (Yang et al., 2024; Jin, 2024). At the same time, studies of security and behavioral biometrics warn against naive federation that would allow cross-platform linkage of behavioral signatures without users' knowledge

(Pfeuffer et al., 2019; Miller et al., 2020; Nair et al., 2023; Rubo et al., 2025), which strengthens the case for strict purpose limitation, on-device processing and governance constraints being built into protocols from the outset.

The governance literature, drawing on platform-governance and public-law perspectives, calls for **"trust-by-design" governance configurations** that combine agile platform-level tools - such as reporting flows, graduated sanctions, real-time prompts and safety-by-default settings - with **external accountability mechanisms** including independent oversight, dispute-resolution bodies and, where appropriate, cooperation with public authorities under robust due-process safeguards (Boellstorff, 2008; Hulkó et al., 2025; Jin, 2024). User-facing commitments - plain-language notices, recognisable iconography for different types of verification, in-world privacy controls and consistent enforcement - are highlighted as key to making norms legible and supporting the kind of boundary coordination envisioned by Communication Privacy Management theory (Petronio, 2002). Moderation and **redress mechanisms** should be proportional, relying in the first instance on local tools such as mute, block and personal-space bubbles, on community moderation and on reversible sanctions, while reserving escalated verification or identity disclosure for clearly delimited serious harms and embedding safeguards against abuse, brigading and structural bias (Yang et al., 2024; Jin, 2024).

From a **measurement and evaluation** perspective, scholars underline that metaverse identity and governance designs should be assessed empirically using **multimodal metrics** that capture user experience, safety and equity. Presence and co-presence can be measured using instruments such as the Presence Questionnaire, the Igroup Presence Questionnaire and related scales (Witmer and Singer, 1998; Schubert et al., 2001; Tran et al., 2024), while comfort and simulator sickness are commonly assessed with the Simulator Sickness Questionnaire and its derivatives (Kennedy, Lane, Berbaum & Lilienthal, 1993; Balk et al., 2013; Bimberg et al., 2020). Trust, disclosure behavior and compliance outcomes - such as harassment incidence, age-restricted-content violations or fraud rates - can be monitored in field experiments and A/B tests as identity policies, verification flows or interface cues are varied (Jin, 2024; Yang et al., 2024; Son et al., 2025). Security-focused work provides methods for quantifying identifiability and inference risks from motion and gaze data (Miller et al., 2020; Pfeuffer et al., 2019; Nair et al., 2023; Rubo et al., 2025; Giaretta, 2025), which can be adapted to evaluate mitigation strategies. Across this emerging body of work, several **research gaps** recur: the need for causal evidence from real-world deployments rather than only lab-based or cross-sectional studies; greater attention to children, teenagers and other vulnerable populations and to how identity and safety arrangements influence their participation; better understanding of cross-border enforcement and interactions between EU instruments and other jurisdictions' regimes; and stronger convergence between technical standardisation efforts by bodies such as W3C, ETSI, CEN/CENELEC and ISO/IEC to reduce fragmentation and compliance ambiguity (W3C, 2022; W3C, 2023; Hulkó et al., 2025; Yang et al., 2024). Overall, the literature portrays **metaverse identity** as a nexus where embodiment, behavioural effects, privacy, biometrics, regulation and technical architecture intersect, and suggests that successful governance will depend on designing identity systems that are interoperable yet privacy-preserving, robust against abuse yet respectful of expression, and grounded both in European regulatory guarantees and in evidence-based assessments of their experiential and distributional impacts.

# 2 Materials and methods

The study was designed as an exploratory experiment to investigate how different metaverse governance configurations and identity policies shape users' perceptions of trust, privacy, openness, presence, and comfort in immersive environments. To capture these dynamics in a controlled yet ecologically valid manner, we employed a virtual reality protocol that combined experimental manipulations with self-report measures administered before and after the immersive experience.

## 2.1 Participants

Participants were recruited at the University of Siena and consisted primarily of undergraduate and postgraduate students between 18 and 28 years of age (56% female). A total of 101 participants completed the study. Recruitment was carried out through institutional mailing lists and classroom announcements, and participation was entirely voluntary. Upon arrival, participants completed a written informed consent form that highlighted their right to withdraw at any time, particularly in the event of discomfort or motion sickness, given the known physiological variability associated with VR exposure. They then filled out a brief demographic questionnaire and a VR literacy scale assessing prior experience with head-mounted displays, gaming, and virtual environments. This measure was later included as a covariate to account for potential differences in baseline VR familiarity. All procedures complied with the relevant institutional guidelines for research involving human participants. Identity verification markers were simulated and not linked to participants' real-world identities or personal data.

## 2.2 Materials and apparatus

Experimental sessions were conducted using Meta Quest headsets (Quest 2 and Quest 3), selected for their portability, reliable tracking, and native integration with mainstream metaverse platforms. Headsets were sanitised before and after each session, and all activities took place in a supervised laboratory space with clearly demarcated boundaries to ensure safe movement.

The virtual environments were implemented on two platforms - Horizon Worlds and VRChat - used as testbeds to instantiate two stylised governance configurations (council-regulated vs. wild-west) and two identity conditions (identity-disclosure cues vs. anonymous interaction). To manipulate governance, we embedded governance cues into the environment and associated interaction interfaces so that regulation was encountered as an ambient, situated property rather than as a purely textual instruction (Boellstorff, 2008; Jin, 2024). In the council-regulated configuration, visual and textual elements emphasised oversight, accountability, recourse, and structured privacy/social controls (e.g., rule and conduct cues,

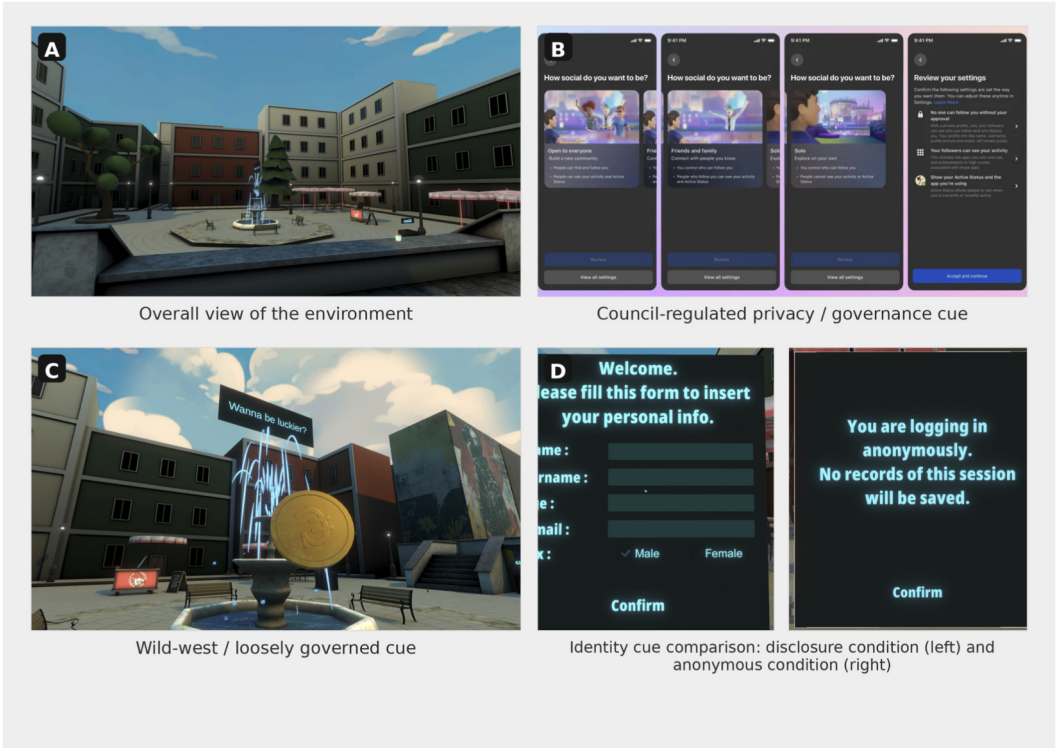



FIGURE 1
Four-panel presentation of the primary governance and identity manipulations. **(A)** Overview of the virtual environment; **(B)** example of the structured privacy/social-control interface used to signal the council-regulated condition; **(C)** example of a wild-west/loosely governed cue from the exploration environment; **(D)** identity-regime cue comparison showing the identity-disclosure prompt (left) and the anonymous login cue (right).

references to moderation and reporting procedures, and reviewable settings or institutional-style assurances about compliance and safeguards). In the wild-west configuration, the environment minimised such cues and presented interaction as loosely governed and less accountable. The identity manipulation varied the degree of identity disclosure requested from participants. In the anonymous conditions, participants interacted through a generic, platform-assigned avatar containing minimal personal information and encountered an anonymous login cue. In the identity-disclosure conditions, participants encountered an in-world personal-information prompt and associated institutional-style disclosure cues intended to simulate a real-name or high-assurance identity regime. These prompts and cues did not correspond to participants' actual identities but were designed to evoke the experiential dimensions of identity verification. To clarify implementation, Figure 1 presents the primary governance and identity cues used to instantiate the four conditions, Figure 2 provides complementary screenshots from the exploration environment, and Figure 3 shows additional task and content cues encountered during exploration.

Where technically feasible, two additional exploratory variations were introduced: visual fidelity (high vs. low rendering detail) and interaction complexity (simple vs. multi-step interactions). Because these variations were limited by platform-level affordances, they were treated as exploratory rather than as fully crossed experimental manipulations.

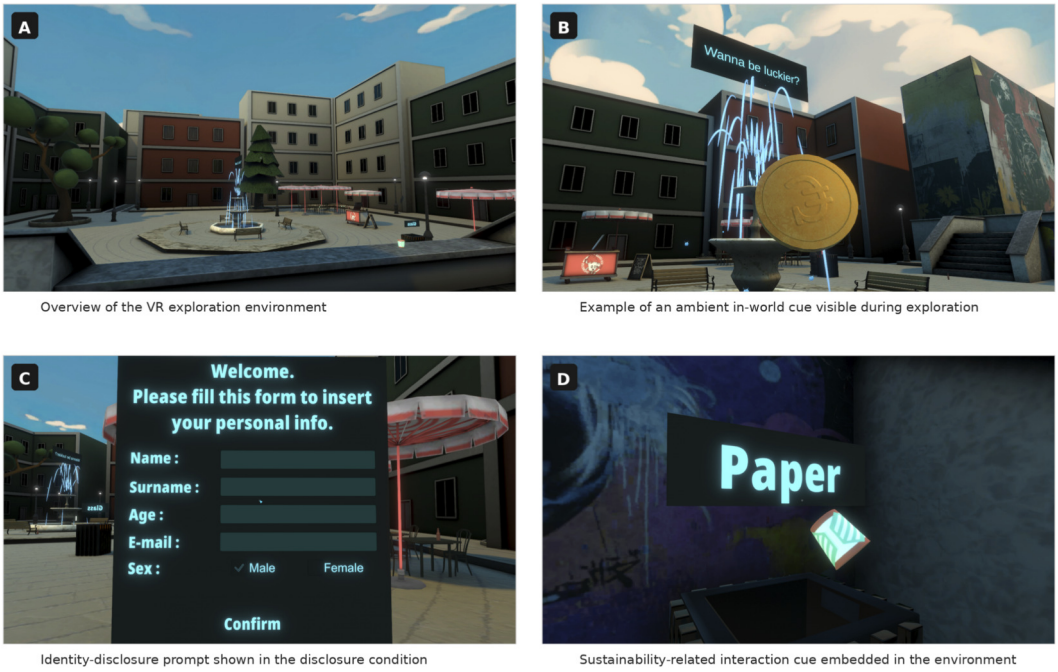
## 2.3 Procedure

Each session followed a standardised structure and lasted approximately 45–60 min. After completing the consent procedure and baseline questionnaires, participants were randomly assigned to one of the four primary experimental conditions defined by the 2 × 2 manipulation of regulatory framework and identity-disclosure cues. Randomisation ensured balanced representation across groups.

Before beginning the main task, participants completed a brief familiarization phase of 10–15 min within a neutral VR environment. This phase allowed them to practice basic navigation and object interaction, ensuring adequate proficiency with the interface while reducing initial disorientation. Participants who experienced notable discomfort at this stage were permitted to withdraw.

The main exploration phase lasted roughly 10–15 min. During this period, participants freely navigated the assigned environment and encountered the governance, identity, and sustainability-related cues associated with their condition (Figures 1–3). They were encouraged to explore naturally—interacting with objects and informational prompts without time constraints or performance requirements. This approach aligned with the study's focus on perceptual, attitudinal, and experiential responses rather than task-based performance.

Immediately after removing the headset, participants completed a battery of post-exposure questionnaires assessing perceived trust



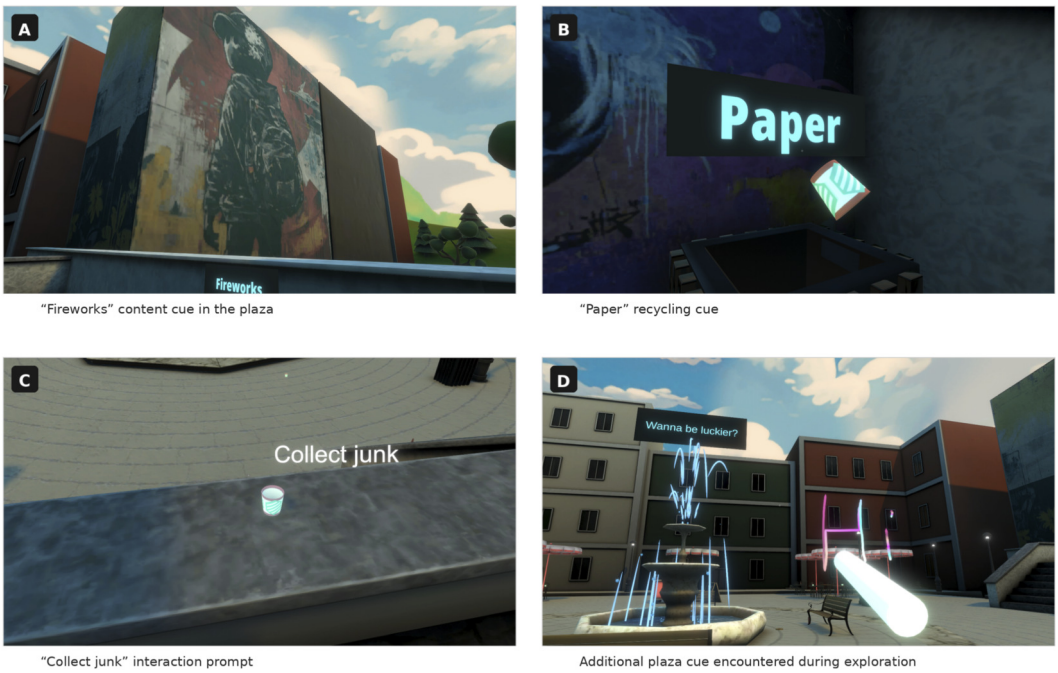

Overview of the VR exploration environment

Example of an ambient in-world cue visible during exploration

Identity-disclosure prompt shown in the disclosure condition

Sustainability-related interaction cue embedded in the environment

FIGURE 2
Complementary screenshot composite from the exploration environment. **(A)** Overview of the VR exploration environment; **(B)** example of an ambient in-world cue visible during navigation; **(C)** close-up of the identity-disclosure prompt shown in the disclosure condition; **(D)** sustainability-related interaction cue embedded in the environment. The identity-disclosure interface was simulated and was not linked to participants' real-world identities.




"Fireworks" content cue in the plaza

"Paper" recycling cue

"Collect junk" interaction prompt

Additional plaza cue encountered during exploration

FIGURE 3
Additional examples of sustainability-related content and interaction cues encountered during exploration. **(A)** "Fireworks" content cue in the plaza; **(B)** "Paper" recycling cue; **(C)** "Collect junk" interaction prompt; **(D)** additional plaza cue encountered during exploration.

and privacy, openness to sustainability-related content, presence and immersion, and overall comfort, including simulator sickness. When session time allowed, additional items on emotional engagement and social presence were administered. Finally, participants received a full debriefing outlining the nature of the experimental manipulations and the broader aims of the study, including its focus on governance and identity-related risks in metaverse environments.

## 2.4 Measures

The primary outcomes of interest were perceived trust, privacy, and openness—constructs closely connected to broader debates on user agency, governance, and sustainable innovation in immersive media. These were assessed using self-report scales administered both before and after VR exposure, allowing for analyses of within-person change and condition-specific effects. Secondary outcomes included presence and immersion, measured with established presence instruments, and simulator sickness, assessed through the Simulator Sickness Questionnaire (Kennedy et al., 1993). Together, these constructs capture core experiential dimensions emphasised in the literature on XR usability, safety, and comfort.

In this study, trust is treated as a user attitude reflecting expectations that the environment and its actors will behave reliably and in good faith, including expectations about how rules are enforced and how personal data are handled. Privacy perceptions refer to participants' subjective appraisal of informational control and contextual appropriateness of data use (Westin, 1967; Nissenbaum, 2010). Because governance cannot be directly observed within a short laboratory exposure, our manipulations target the perceived regulated environment - that is, the extent to which oversight, accountability, and recourse are made legible through in-world cues and procedural affordances. We therefore distinguish governance (institutional arrangements and enforcement capacity), regulated environment (user-facing signals and interaction mechanisms), and trust (an attitudinal outcome shaped by both).

In a subset of sessions, system logs capturing behavioural indicators such as movement trajectories and interaction counts were also recorded, though these data were used primarily for exploratory analysis. When time permitted, participants additionally completed optional measures of emotional and social presence to provide a more nuanced characterisation of the experiential profile associated with each condition.

## 2.5 Statistical analysis

Data analysis proceeded in several stages. Mixed-effects ANOVA models were used to examine the main effects of regulatory framework and identity condition on the primary outcome variables, with VR literacy included as a covariate. Visual fidelity and interaction complexity were incorporated as exploratory factors but were not treated as primary drivers of the results due to their limited implementation across conditions.

To evaluate overall shifts in trust and privacy perceptions from pre-to post-exposure, paired-samples t-tests were conducted on the full sample. Zero-order correlations among the primary outcome variables were computed to examine associations among trust, privacy, openness, presence, and comfort. Finally, qualitative comments collected during the debriefing were reviewed to contextualise the quantitative findings and to identify themes related to participants' perceptions of governance, identity, and risk in immersive environments.

# 3 Results

## 3.1 Sample characteristics and data quality

A total of 101 participants completed both pre- and post-test measures. The sample was well-balanced across experimental conditions, with 25 participants in the council-regulated with identity-disclosure condition (Vrc-id), 25 in the council-regulated without identity disclosure condition (Vrc-noid), 26 in the wild-west with identity-disclosure condition (W-id), and 25 in the wild-west without identity disclosure condition (W-noid).

## 3.2 Scale reliability and data cleaning

Prior to conducting the main analyses, comprehensive data screening was performed to ensure the integrity and reliability of all measurement instruments. This process involved systematic examination of item-level characteristics and correction of methodological artefacts that could compromise the validity of subsequent analyses.

Two critical issues were identified and addressed during the data cleaning process. First, twelve questionnaire items demonstrated zero variance, with all 101 participants providing identical responses. This included nine items from the Igroup Presence Questionnaire (IPQ) and three items from the baseline privacy scale. Items with zero variance cannot discriminate among participants, fail to correlate with other variables, and artificially inflate reliability estimates while adding only a constant to total scores. These items were therefore excluded from both reliability calculations and scale score computations.

Second, reverse-keyed items required recoding to ensure consistent directionality across all measures. Four IPQ items (items 5, 6, 10, and 12) and three baseline privacy items (items 1, 4, and 6) were negatively worded and required response scale inversion (e.g., transforming responses of 1→7, 2→6) so that higher values consistently indicated greater levels of the target construct. Following these data cleaning procedures, reliability analyses were conducted for all scales using Cronbach's alpha. The results revealed substantial variation in internal consistency across measures, as presented in Table 1.

However, two scales showed concerning reliability patterns. The baseline privacy scale, after removing zero-variance items, yielded a negative alpha coefficient ($\alpha = -0.09$), indicating that the remaining three items did not form a coherent construct in this sample. Similarly, the presence scale reliability dropped substantially from the original 13 items to just four informative items, resulting in low internal consistency ($\alpha = 0.24$). These low reliability values suggest that the pilot sample demonstrated limited variability on these particular constructs. However, the cleaned scores remain statistically defensible and free from constant-item artefacts.

TABLE 1 Scale reliability and item retention.

| Scale | Items retained | Cronbach's α | Reliability assessment |
|---|---|---|---|
| VR literacy (pre-test) | 6/6 | 0.84 | Good |
| Baseline privacy (pre-test) | 3/6 | −0.09 | Unreliable |
| Trust/Privacy (post-test) | 6/6 | 0.63 | Acceptable |
| Openness (post-test) | 6/6 | 0.77 | Good |
| Presence (post-test) | 4/13 | 0.24 | Low |
| Simulator sickness (post-test) | 16/16 | 0.91 | Excellent |

The VR literacy scale demonstrated good reliability (α = .84) with all six original items retained. The simulator sickness questionnaire showed excellent internal consistency (α = .91) with all 16 items contributing meaningfully to the scale. The openness scale demonstrated good reliability (α = .77), while the trust/privacy scale achieved acceptable levels of reliability (α = .63).

TABLE 2 Paired t-test summary (pre to post trust/privacy).

| Statistic | Value |
|---|---|
| Mean difference | −0.49 |
| t | −3.701 |
| df | 100 |
| p-value | 0.000352 |
| 95% CI lower | −0.753 |
| 95% CI upper | −0.227 |
| Cohen's d | 0.528 |

## 3.3 Pre-post changes in trust and privacy perceptions and effects of manipulations

To examine whether the virtual reality experience influenced participants' trust and privacy perceptions, a paired-samples t-test compared pre-test and post-test scores on the trust/privacy measure. Post-test trust/privacy ratings were significantly higher than pre-test ratings (mean difference pre minus post = −0.49, 95% CI [-0.75, −0.23]), t(100) = −3.70, $p < 0.001$, Cohen's d = 0.53 (Table 2). This represents a medium-sized effect, indicating that participants generally reported enhanced trust and privacy perceptions after engaging with the virtual environment, regardless of experimental condition.

The primary research questions focused on the differential effects of regulatory frameworks (council-regulated vs. wild-west) and identity conditions (identity-disclosure cues vs. anonymous interaction) on various aspects of the VR experience. These effects were examined using a series of 2 × 2 analysis of covariance (ANCOVA) models, with VR literacy included as a covariate to control for individual differences in virtual reality familiarity and expertise. Model coefficients are summarised in Table 3.

The ANCOVA examining trust and privacy perceptions revealed a significant main effect of regulatory framework, F(1, 96) = 5.02, p = 0.027. Participants in council-regulated virtual worlds reported significantly higher levels of trust and privacy compared to those in wild-west environments. The identity-condition manipulation did not produce a significant main effect, F(1, 96) = 0.25, p = 0.618, nor was there a significant interaction between regulatory framework and identity condition, F(1, 96) = 0.10, p = 0.754. The VR literacy covariate was not significantly related to trust and privacy outcomes, F(1, 96) = 0.05, p = 0.828.

Analysis of openness and sustainability attitudes showed no significant effects of either experimental manipulation. The regulatory framework main effect was not significant, F(1, 96) = 1.87, p = 0.175, nor was the identity-condition main effect, F(1, 96) = 0.71, p = 0.401. The interaction between these factors was also non-significant, F(1, 96) = 0.01, p = 0.938. VR literacy did not significantly predict openness attitudes, F(1, 96) = 1.37, p = 0.245.

The analysis of simulator sickness revealed a highly significant main effect of regulatory framework, F(1, 96) = 10.70, p = 0.001. Participants in council-regulated environments experienced substantially lower levels of simulator sickness compared to those in wild-west conditions. This effect was particularly notable given its large magnitude, with council-regulated worlds reducing simulator

TABLE 3 ANCOVA results (standardized beta with p-value in parentheses).

| Predictor | Trust/Privacy | Openness | Simulator sickness | Presence |
|---|---|---|---|---|
| Regulatory [W] | −0.61 (0.027) | −0.38 (0.175) | 0.85 (0.001) | −0.22 (0.438) |
| Identity [noid] | 0.14 (0.617) | 0.24 (0.401) | −0.30 (0.259) | −0.62 (0.030) |
| Regulatory [W] × identity [noid] | 0.12 (0.754) | 0.03 (0.938) | −0.21 (0.560) | 0.33 (0.408) |
| VR lit | 0.02 (0.828) | 0.12 (0.245) | −0.01 (0.884) | 0.06 (0.521) |
| R2/R2 adjusted | 0.089/0.051 | 0.062/0.023 | 0.183/0.149 | 0.064/0.025 |

Entries are standardised betas; p-values are in parentheses. Reference categories: Regulatory, Vrc (council-regulated); Identity, id (identity-disclosure cues). N = 101.

10.3389/frvir.2026.1779260

TABLE 4 Intercorrelations among primary outcome variables.

| Variable | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1. VR literacy** | - | **0.02** | **0.11** | **0.07** | **0.00** |
| **2. Trust/Privacy** | | - | **0.61*** ** | **−0.26**** | **−0.43***** |
| **3. Openness** | | | - | **−0.09** | **−0.14** |
| **4. Presence** | | | | - | 0.32*** |
| **5. Simulator sickness** | | | | | - |

Bold values indicate statistically significant correlations. **p < 0.01; ***p < 0.001.

sickness scores by approximately half relative to unregulated environments. Neither the identity-condition main effect, $F(1, 96) = 1.29$, $p = 0.259$, nor the regulatory framework × identity condition interaction, $F(1, 96) = 0.34$, $p = 0.560$, reached statistical significance. VR literacy was unrelated to simulator sickness, $F(1, 96) = 0.02$, $p = 0.884$.

The spatial presence analysis yielded a significant main effect of identity condition, $F(1, 96) = 4.85$, $p = 0.030$. Participants who could interact anonymously reported lower levels of spatial presence compared to those in the identity-disclosure condition (beta = −0.62, $p = 0.030$; Table 3). The main effect of the regulatory framework was not significant, $F(1, 96) = 0.61$, $p = 0.438$, nor was the interaction between the regulatory framework and identity condition, $F(1, 96) = 0.69$, $p = 0.408$. VR literacy did not significantly predict spatial presence, $F(1, 96) = 0.41$, $p = 0.521$.

## 3.4 Correlational patterns among outcome variables

Zero-order correlations among the primary outcome variables revealed several meaningful associations that provide insight into the relationships between different aspects of the VR experience (Table 4).

The strongest correlation emerged between trust/privacy and openness ($r = 0.61$, $p < 0.001$), suggesting that participants who felt more secure and trusted in the virtual environment were also more open to sustainability-related concepts and behaviours. Trust and privacy perceptions were negatively correlated with simulator sickness ($r = −0.43$, $p < 0.001$), indicating that participants who experienced greater comfort and security in the virtual environment were less likely to experience adverse physiological symptoms.

Interestingly, spatial presence showed a positive correlation with simulator sickness ($r = 0.32$, $p < 0.001$), suggesting that more immersive experiences may come at the cost of increased physiological discomfort. Presence was negatively correlated with trust and privacy perceptions ($r = −0.26$, $p = 0.01$), indicating a potential trade-off between immersive engagement and feelings of security within the virtual environment.

VR literacy showed minimal correlations with all outcome variables, with correlation coefficients ranging from 0.00 to 0.11, none of which reached statistical significance. This pattern is consistent with the ANCOVA results showing that VR literacy was not a significant predictor in any of the experimental models.

The experimental manipulation of the regulatory framework emerged as the most consistent and impactful factor influencing the quality of the VR experience. Council-regulated virtual worlds produced two major benefits: significantly enhanced trust and privacy perceptions and dramatically reduced simulator sickness compared to wild-west environments. The magnitude of the simulator sickness reduction was substantial, with regulated environments cutting adverse symptoms by approximately half.

The identity-condition manipulation showed a more selective pattern of effects. While the identity-disclosure condition did not influence trust, openness, or simulator sickness, it did produce a reliable increase in spatial presence relative to anonymous interaction. This suggests that identity-disclosure cues (even when simulated) may facilitate a stronger sense of 'being there', even when they do not affect other aspects of user experience or comfort.

Notably, no significant interactions emerged between regulatory framework and identity condition across any outcome measure, indicating that these factors operate independently rather than synergistically. The VR literacy covariate consistently failed to predict any outcome variables, suggesting that individual differences in virtual reality experience and expertise did not meaningfully influence responses to the experimental manipulations in this sample.

The correlational analyses revealed a coherent pattern of relationships among outcome variables, with trust and privacy serving as a central hub connecting to multiple other aspects of the VR experience. The strong positive correlation between trust and openness suggests that creating secure virtual environments may facilitate greater receptivity to educational or persuasive content. Conversely, the negative correlations between trust and both simulator sickness and spatial presence highlight potential tensions in VR design, where maximising immersion or minimising discomfort may require careful balance with security and privacy considerations.

# 4 Discussion

The present study provides exploratory empirical evidence on how governance and identity are experienced in immersive virtual environments. By contrasting a council-regulated configuration with a comparatively 'wild-west' configuration, and by varying whether users encountered identity-disclosure cues versus interacting anonymously, we assessed effects on perceived trust and privacy, openness to sustainability-related content, spatial presence, and simulator sickness. Across outcomes, the most robust pattern was that governance cues - rather than identity condition *per se* - shifted participants' experience: regulated environments elicited higher trust/privacy ratings and substantially lower simulator sickness. Identity condition, in turn, showed a narrower experiential footprint: anonymity was associated with lower spatial presence, while trust/privacy, openness, and sickness were largely unaffected. Although correlational patterns should not be interpreted causally, the results also suggest that trust/privacy may function as a central experiential node connecting openness, comfort, and immersion.

The finding that a council-regulated environment increased perceived trust and privacy aligns with governance research that emphasises "trust-by-design" configurations, where user-facing commitments (clear rules, predictable enforcement, and visible

accountability) complement back-end moderation and oversight (Boellstorff, 2008; Jin, 2024; Hulkó et al., 2025). Importantly, as illustrated in Figures 1, 2, our manipulation relied primarily on visible signalling and interface-level cues—rather than on technologically enforced changes to data flows—yet still produced measurable differences in perceived legitimacy. This supports the claim that, in XR, governance is not encountered only as terms-of-service text but as an ambient property of the environment and associated interfaces: iconography, institutional references, structured privacy/social settings, disclosure prompts, and procedural affordances can calibrate expectations about how misconduct is handled, which norms apply, and what recourse is available.

From a privacy-theory perspective, such cues may operate by reshaping the "privacy calculus" (Dinev and Hart, 2006) and contextual expectations about appropriate information flows (Nissenbaum, 2010). When the environment is framed as rule-governed and accountable, users may infer tighter purpose limitation, more constrained secondary uses of telemetry, and clearer role boundaries—assumptions that can reduce perceived risk even when the underlying technical stack is not directly observable. The result is consistent with Communication Privacy Management theory's emphasis on the need for legible boundary rules once information is shared in a relationship or community (Petronio and Child, 2020): governance cues effectively communicate what those boundary rules are supposed to be.

The same mechanism may also help explain the large reduction in simulator sickness observed in the regulated condition. Simulator sickness is typically treated as a function of sensory conflict, locomotion, and display characteristics (Kennedy et al., 1993; Bimberg et al., 2020), but user state—including arousal, vigilance, and perceived control—can modulate how discomfort is experienced and reported. If governance cues reduce uncertainty about social and informational risk, participants may be less vigilant and more relaxed, which in turn could lower reported sickness. This is a hypothesis that requires direct testing, but it illustrates a broader point: "comfort" in VR may not be reducible to rendering and locomotion alone; it may also be shaped by socio-technical assurances that make environments feel safe and predictable.

Experimentally, because governance was operationalised through environmental framing and in-world interface cues, the sickness effect could also reflect expectancy mechanisms: a space signalled as governed and safe may reduce anticipatory anxiety and interoceptive focus, while a space framed as unregulated may heighten vigilance and symptom monitoring. Epistemologically, this underscores that SSQ responses are not purely physiological readouts but are mediated by interpretation and meaning-making in context (Balk et al., 2013). Semantically, the governance manipulation may have carried connotations of professionalism, legitimacy, and predictability that overlap with comfort-related judgements. Future work should triangulate SSQ with objective comfort metrics (e.g., postural sway, head-movement patterns) and manipulate governance cues independently of technical comfort settings to disentangle socio-semantic framing from locomotion and display effects.

The identity-disclosure condition did not raise trust/privacy ratings in this study, but it did increase spatial presence relative to anonymous interaction. One plausible interpretation is that identity cues (e.g., disclosure prompts or verification markers) increase self-relevance and social realism, supporting avatar identification and embodied engagement. This interpretation is consistent with prior work showing that identity presentation and avatar affordances can shape self-perception and behaviour (Yee and Bailenson, 2007; Yee et al., 2009; Coesel, 2024). At the same time, this presence effect should be interpreted cautiously because the reduced presence scale showed low internal consistency in this pilot; future studies should replicate the finding with more reliable presence instruments and complementary behavioural or physiological indicators.

At the same time, the absence of a trust gain cautions against assuming that stronger disclosure or real-name policies automatically deliver felt safety. Real-name disclosure can increase accountability for certain forms of abuse, but it can also chill expression and heighten exposure to offline harms (e.g., doxxing or cross-context profiling), especially when telemetry and biometrics make linkage across sessions and services feasible (Pfeuffer et al., 2019; Miller et al., 2020; Nair et al., 2023; Rubo et al., 2025). The present results therefore support the growing argument for hybrid identity regimes: pseudonymity as a default for everyday interaction, combined with selective, context-specific verification for high-stakes contexts such as payments, age-restricted spaces, or serious misconduct investigation (W3C, 2022; W3C, 2023; European Parliament and Council, 2024b). Such designs can preserve experiential affordances associated with anonymity while still enabling proportionate, due-process accountability when needed.

The experimental manipulations did not directly affect openness to sustainability-related content, but openness was strongly associated with trust/privacy. This pattern suggests that perceived safety and legitimacy may be a precondition for receptivity to educational, civic, or pro-social messaging in immersive settings. For initiatives aiming to use VR for public-interest goals—such as sustainability education, participation, and social innovation—designing for trustworthy governance may therefore be as important as content design. The lack of a direct manipulation effect could reflect the brief, low-stakes exposure and the absence of consequential decisions in the protocol; more behaviourally grounded tasks (e.g., choices involving disclosure, volunteering, or resource allocation) may be required to detect governance-related changes in openness.

The correlational structure of outcomes points to potential experiential trade-offs. Trust/privacy was negatively associated with both simulator sickness and spatial presence, while presence was positively associated with simulator sickness. One interpretation is that environments experienced as highly immersive may also be more physiologically demanding, and that heightened sensory engagement can coexist with increased discomfort (Kennedy et al., 1993). Conversely, environments that feel more governed and controlled may encourage a calmer, more comfort-oriented interaction style, which could dampen immersion. However, these correlations should be interpreted cautiously given the low internal consistency of the reduced presence scale in this pilot. Future studies should replicate these relationships with more reliable presence instruments and, where possible, triangulate self-report with behavioural and physiological indicators (e.g., postural instability, gaze behaviour, and locomotion patterns).

Two measurement issues are especially salient for XR research on governance and identity. Firstly, the baseline privacy scale showed very low reliability after removing zero-variance items, which constrains the interpretability of pre–post changes in privacy-related perceptions. Secondly, the substantial item reduction required for the IPQ presence scale resulted in low internal consistency, limiting confidence in effect-size estimates involving presence. Both issues suggest that standard questionnaires may not transfer cleanly to short, stylised metaverse exposures, where participants may interpret items differently or exhibit restricted response ranges. Developing and validating XR-specific instruments for perceived privacy, governance legitimacy, and identity-related comfort—potentially grounded in contextual-integrity constructs and concrete interface experiences—should be a priority for future work.

Several limitations qualify the conclusions. The sample was relatively young and homogeneous, limiting generalisability to older populations, minors, or users with different cultural and risk profiles. The exposure was brief and low-stakes, and participants interacted primarily in an exploratory mode; effects on disclosure behaviour, norm compliance, or sustained participation may differ in longer-term, socially dense metaverse settings. The governance and identity manipulations were necessarily stylised and may not capture the full complexity of real deployments, where moderation capacity, enforcement consistency, and technical controls (e.g., data minimisation, on-device processing) jointly shape experience.

In addition, the regulatory conditions were operationalised through commercially available platforms, which introduces the possibility that unmeasured platform differences (e.g., locomotion defaults, performance stability, interface conventions, procedural affordances such as reporting tools or comfort modes, or aesthetic fidelity) contributed to the observed effects. Although visual fidelity and interaction complexity were treated as exploratory factors, they were not fully crossed with the primary manipulations. Replication within a single platform using controlled world-building, or across multiple platforms with matched interaction and comfort settings, will be important to isolate governance signalling from platform-specific confounds.

## 5 Conclusion

Despite these constraints, the results offer actionable implications for both platform design and policy discussions around open, human-centric virtual worlds. Firstly, governance should be made legible in-world: users need recognisable cues that communicate oversight, reporting pathways, and enforcement consistency, ideally coupled with accessible explanations of what telemetry is collected and for which purposes. Secondly, identity systems should be proportionate and context-sensitive. Rather than default real-name disclosure, platforms can adopt graduated verification that supports pseudonymous participation while enabling attribute-based access control (e.g., age or role claims) through verifiable credentials and selective disclosure (W3C, 2022; W3C, 2023; European Parliament and Council, 2024b). Thirdly, user comfort should be treated as a socio-technical outcome: design interventions that increase perceived control and accountability may contribute to reductions in discomfort alongside technical comfort modes.

Future research can build on these findings by (i) experimentally disentangling signaling from enforcement (e.g., comparing symbolic compliance cues with active safety-by-design features), (ii) testing more granular identity regimes (e.g., tiered verification, temporary pseudonyms, or role-based credentials), (iii) incorporating richer behavioural and physiological measures, and (iv) moving beyond lab pilots to field experiments and longitudinal designs that capture how trust, privacy, and presence evolve with community norms and repeated exposure. Such work would directly support roadmaps—such as those developed within OPENVERSE—that aim to operationalise openness and interoperability without sacrificing fundamental rights or user wellbeing.

Overall, the study reinforces that metaverse governance and identity design are not abstract legal layers sitting outside the experience. Even minimal changes in how rules and identity are framed can alter how safe, comfortable, and engaged users feel in VR. Designing virtual worlds that are both experientially rich and rights-respecting will require integrating governance legibility, proportionate identity, and comfort-by-design as co-equal elements of the immersive stack.

## Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

## Ethics statement

The studies involving humans were approved by Ethics Committee for Research in the Human and Social Sciences CAREUS of the University of Siena. The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

## Author contributions

GAV: Conceptualization, Supervision, Methodology, Writing – original draft, Formal Analysis. FM: Funding acquisition, Supervision, Resources, Writing – original draft, Project administration. AI: Data curation, Writing – review and editing, Methodology, Writing – original draft. MS: Writing – original draft, Software, Visualization. EV: Writing – original draft, Data curation.

## Funding

The author(s) declared that financial support was received for this work and/or its publication. Funding and responsibility disclaimer. This work has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101135701 (OPENVERSE). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or

the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

## Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Generative AI statement

The author(s) declared that generative AI was used in the creation of this manuscript. Improvement of the draft in English.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

## Publisher's note



## References

Balk, S. A., Bertola, M. A., and Inman, V. W. (2013). "Simulator sickness questionnaire: twenty years later," in *Proceedings of the seventh international driving symposium on human factors in driver assessment*, 257–263.

Bimberg, P., Weissker, T., and Magnor, M. A. (2020). On the usage of the simulator sickness questionnaire for virtual reality research. arXiv:2008.06460.

Biocca, F., and Harms, C. (2002). *Networked minds social presence inventory: measures of co-presence, social presence, subjective and intersubjective symmetry*. East Lansing, MI: Media Interface and Network Design (M.I.N.D.) Lab, Michigan State University.

Boellstorff, T. (2008). *Coming of age in second life: an anthropologist explores the virtually human*. Princeton University Press.

Coesel, A. M., Biancardi, B., and Buisine, S. (2024). A theoretical review of the proteus effect: understanding the underlying processes. *Front. Psychol.* 15, 1379599. doi:10.3389/fpsyg.2024.1379599

Dinev, T., and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* 17 (1), 61–80. doi:10.1287/isre.1060.0080

European Parliament and Council (2016). Regulation (EU) 2016/679 (general data protection regulation). *Official J. Eur. Union*. 119, 1–88. Available online at: http://data.europa.eu/eli/reg/2016/679/oj.

European Parliament and Council (2022a). Regulation (EU) 2022/1925 (digital markets act). *Official J. Eur. Union*. 265, 1–66. Available online at: http://data.europa.eu/eli/reg/2022/1925/oj.

European Parliament and Council (2022b). Regulation (EU) 2022/2065 (digital services act). *Official J. Eur. Union*. 277, 1–102. Available online at: http://data.europa.eu/eli/reg/2022/2065/oj.

European Parliament and Council (2024a). Regulation (EU) 2024/1689 (artificial intelligence act). *Official J. Eur. Union*. Available online at: http://data.europa.eu/eli/reg/2024/1689/oj.

European Parliament and Council (2024b). Regulation (EU) 2024/1183 amending regulation (EU) no 910/2014 (eIDAS 2.0). *Official J. Eur. Union*. Available online at: http://data.europa.eu/eli/reg/2024/1183/oj.

Giaretta, A. (2025). Security and privacy in virtual reality: a literature survey. *Virtual Real.* 29, 10. doi:10.1007/s10055-024-01079-9

Hulkó, G., Kálmán, J., and Lapsánszky, A. (2025). The politics of digital sovereignty and the european Union's legislation: navigating crises. *Front. Political Sci.* 7, 1548562. doi:10.3389/fpos.2025.1548562

Jin, S. V. (2024). In the metaverse we (Mis)trust? *Cyberpsychology, Behav. Soc. Netw.* 27 (1), 64–75. doi:10.1089/cyber.2022.0376

Kennedy, R. S., Lane, N. E., Berbaum, K. S., and Lilienthal, M. (1993). Simulator sickness questionnaire: an enhanced method for quantifying simulator sickness. *Int. J. Aviat. Psychol.* 3 (3), 203–220. doi:10.1207/s15327108ijap0303_3

Miller, M. R., Herrera, F., Jun, H., Landay, J. A., and Bailenson, J. N. (2020). Personal identifiability of user tracking data during observation of 360° VR video. *Sci. Rep.* 10, 17404. doi:10.1038/s41598-020-74486-y

Nair, V., Williams, E., and Gehring, S. (2023). "Unique identification of 50,000+ virtual reality users from head and hand motion data," in *USENIX security '23*.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford University Press.

Petronio, S. (2002). Boundaries of privacy: dialectics of disclosure. Albany, NY: State University of New York Press.

Petronio, S., and Child, J. T. (2020). Conceptualization and operationalization: utility of communication privacy management theory. *Curr. Opin. Psychol.* 31, 76–82. doi:10.1016/j.copsyc.2019.08.009

Pfeuffer, K., Geiger, M. J., Prange, S., Mecke, L., Buschek, D., and Alt, F. (2019). "Behavioural biometrics in VR: identifying people from body motion and relations in virtual reality", in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19), New York, NY: Association for Computing Machinery. 1–12. doi:10.1145/3290605.3300340

Ratan, R., Beyea, D., Li, B. J., and Graciano, L. (2020). Avatar characteristics induce users' behavioral conformity via the proteus effect. *Media Psychol.* 23 (1), 1–25. doi:10.1080/15213269.2019.1623698

Rubo, M., and Son, G. (2025). Social gaze fingerprints: identifying social VR users via eye-gaze. *Virtual Real.* 29. doi:10.1007/s10055-025-01210-4

Schubert, T., Friedmann, F., and Regenbrecht, H. (2001). *The igroup presence questionnaire (IPQ)*.

Short, J., Williams, E., and Christie, B. (1976). *The social psychology of telecommunications*. Wiley.

Son, G., Tiemann, A., and Rubo, M. (2025). I am here with you: an examination of factors relating to social presence in social VR. *Front. Virtual Real.* 6, 1558233. doi:10.3389/frvir.2025.1558233

Tran, T. Q., Langlotz, T., Young, J., Schubert, T. W., and Regenbrecht, H. (2024). Classifying presence scores: insights from two decades of the IPQ. *ACM Trans. Computer–Human Interact.* 31 (5), 1–26. doi:10.1145/3689046

Turkle, S. (1995). *Life on the screen: identity in the age of the internet*. New York, NY: Simon and Schuster.

W3C (2022). *Decentralized identifiers (DIDs) v1.0. W3C recommendation*.

W3C (2023). *Verifiable credentials data model v2.0. W3C recommendation*.

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Witmer, B. G., and Singer, M. J. (1998). Measuring presence in virtual environments: a presence questionnaire. *Presence* 7 (3), 225–240. doi:10.1162/105474698565686

Yang, L., Xu, Y., and Hui, P. (2024). Metaverse identity: core principles and critical challenges. arXiv:2406.08029.

Yee, N., and Bailenson, J. (2007). The proteus effect: the effect of transformed self-representation on behavior. *Hum. Commun. Res.* 33 (3), 271–290. doi:10.1111/j.1468-2958.2007.00299.x

Yee, N., Bailenson, J., and Ducheneaut, N. (2009). The proteus effect in full-body avatars. *Commun. Res.* 36 (2), 285–312. doi:10.1177/0093650208330254