Qwen

A Comprehensive Architectural Blueprint for Reality.os: Enforcing Neuro-Rights in Immersive Computing

Foundational Architecture for Sovereign Data Control and Neuro-Rights Enforcement

The foundational architecture of Reality.os is predicated on the principle of user sovereignty over neural, biometric, environmental, and interaction data user]]. This requires a multi-layered approach combining cryptographic guarantees, granular consent management, and a tamper-proof record of all data-related activities. The core mechanism for ensuring data ownership is the adoption of a local-first, encrypted vault model where all sensitive information resides by default on the user's device user]]. This directly counters the pervasive industry practice where consumer neurotechnology companies take possession of users' neural data, often retaining unfettered access rights and permitting broad third-party sharing without meaningful limitations [4,97]. To operationalize this, Reality.os must employ robust end-to-end encryption for data at rest and in transit, leveraging modern algorithms capable of resisting both classical and future quantum computing threats, such as lattice-based post-quantum cryptography (PQC) [58]. The architecture should also incorporate advanced privacy-preserving computation techniques like homomorphic encryption (HE), which allows for certain computations to be performed on encrypted data without decrypting it first, thereby minimizing exposure of raw data during processing [56,92].

Central to enforcing neuro-rights is the concept of dynamic, granular consent. Static, one-time opt-in agreements are insufficient and easily circumvented through manipulative interface design, or "dark patterns" [94]. Reality.os must therefore implement a sophisticated consent management framework that moves beyond simple binary choices. This involves creating clear, tiered options for data usage—for instance, allowing a user to permit EEG analysis only for seizure detection while explicitly prohibiting its use for mood analysis [45]. Consent must be actively renewable, and any attempt to alter the purpose of data processing beyond the originally agreed-upon scope must trigger a new, explicit consent request from the user [15]. This aligns with the principles of the EU AI Act, which mandates transparency and human oversight for high-risk systems, and California's SB 1223, which classifies neural data as sensitive personal information requiring opt-in consent before collection [43,45]. To provide auditable proof of neuro-rights compliance, all consents and data access events must be logged in a secure, append-only ledger user]]. This can be implemented using a lightweight blockchain or a formally verified distributed ledger technology, ensuring that every access request, whether from an application, a framework, or a cross-platform feature, is permanently recorded and cannot be altered or deleted [37]. This ledger serves as an immutable audit trail, providing users with full transparency into who accessed their data and for what purpose, a critical requirement for building trust and enabling regulatory compliance [16].

The mapping of these architectural controls to the five priority neuro-rights provides a clear enforcement strategy. For Mental Privacy, the combination of on-device encryption and strict API gating ensures that private thoughts, emotions, and mental states remain inaccessible without explicit, verifiable user consent [2,14]. The secure consent ledger logs every instance of data access, creating a transparent record of compliance . For Cognitive Liberty, the architecture supports user override workflows and opt-out mechanisms, empowering individuals to control or reject cognitive augmentation and neural stimulation [7,40]. This is further reinforced by mandatory explicit consent screens for any action that could influence cognitive state, preventing covert manipulation [94]. The right to Identity Integrity is protected by implementing robust anti-spoofing measures and active monitoring of identity-related sessions . Given that brainwave patterns ("brainprints") can identify individuals with over 90% accuracy [14,91], and that biometric authentication systems are vulnerable to presentation attacks [48], Reality.os must integrate liveness detection technologies that analyze pupil response, skin texture, and other physiological signals to distinguish between a live person and a digital replica [50,54]. This proactive defense is crucial for preventing unauthorized identity alteration or spoofing in shared virtual environments . Finally, Agency/Free Will is guaranteed through mandatory user confirmation for all significant actions, especially those involving data sharing or irreversible system changes . This ensures that users retain absolute control over their decisions, a principle echoed in regulations that invalidate consent obtained through manipulative interfaces [94]. Fair Access & Algorithmic Bias Protection is addressed by incorporating bias detection heuristics within the data processing pipelines and maintaining comprehensive audit trails that allow for independent auditing of algorithmic decision-making processes, ensuring that AR/VR enhancements and neuromorphic upgrades are equitable and non-discriminatory [2].

Neuro-Right Priority	Key Enforcement Mechanism	Supporting Technical Controls	Relevant Policy/Legal Framework
Mental Privacy	Strict API Gating & Granular Consent	On-device End-to-End Encryption, Homomorphic Encryption (HE), Secure Append-Only Ledger [37,56,58]	EU GDPR (Article 9), California SB 1223, Colorado HB24-1058, Chilean Constitution [15,45,102]
Cognitive Liberty	Active User Override & Opt-Out Workflows	Dynamic Consent Models, Mandatory Explicit Consent Screens, Prohibition of Subliminal Manipulation [15,42,94]	EU AI Act (Prohibited Practices), Habeas Cogitationem Writ, OECD Responsible Innovation Principles [16,40,43]
Identity Integrity	Biometric Integrity Checks & Anti-Spoofing	Liveness Detection (Pupil Response, Skin Texture),	Council of Europe Oviedo Convention, UN Declaration on Bioethics [21,100]

Neuro-Right Priority	Key Enforcement Mechanism	Supporting Technical Controls	Relevant Policy/Legal Framework
		Zero-Knowledge Proofs (ZKPs), Secure Enclaves [50 54 58]	
Agency/ Free Will	Mandatory Explicit Confirmation & Overrides	Human-in-the-Loop Oversight, Explainable AI (XAI) Dashboards, Clear Revocation Rights [46 47]	OECD AI Principles, NIST AI RMF, Chilean Constitutional Neurorights [16]
Fair Access/ Bias	Audit Trails & Bias Detection Heuristics	Federated Learning (FL), Differential Privacy, Bias Auditing Algorithms [46 56 92]	EU AI Act (High-Risk Systems), UN Ethical Guidelines for BCI Research [15 43]

Security Framework Separation and Hardened System Isolation

To create a truly secure environment for handling sensitive neural and biometric data, Reality.os must adopt a defense-in-depth strategy centered on strict security framework separation. The proposal to run all VR/AR environments, applications, and neuromorphic services in sandboxed containers with OS-level capability management and zero implicit trust is a fundamental security best practice user]]. This model confines each application's execution space, preventing a compromised or malicious app from accessing resources outside its designated boundary or interfering with other applications and the core OS [109]. In the context of XR, where developers often exhibit significant awareness gaps regarding security threats like software side-channels and perception attacks, this isolation is paramount [57]. Sandboxing limits the blast radius of any potential vulnerability, ensuring that even if an application is exploited, it cannot exfiltrate user data or cause system-wide harm. This aligns with the security architectures of enterprise-grade devices like Microsoft HoloLens 2, which uses strong application sandboxing and UEFI Secure Boot to prevent runtime compromise and ensure only trusted software executes [107 108].

The most critical component of Reality.os's architecture is the use of formally verified kernels for all trusted core OS functions user]]. This elevates the security posture beyond conventional software engineering practices. A formally verified kernel, such as seL4, is accompanied by a mathematical proof that its implementation adheres strictly to its security specification. This provides an unprecedented level of assurance that the kernel itself is free from common vulnerabilities like buffer overflows, race conditions, and memory corruption bugs that could be exploited to escalate privileges and gain unauthorized access to sensitive data [58]. By running the most privileged parts of the OS, such as the hardware abstraction layer and inter-process communication manager, within this provably secure microkernel, Reality.os can establish an unbreachable foundation. All other components, including the main VR/AR runtime and third-party applications, would operate in more permissive sandboxes, but their ability to interact with the kernel and access hardware is strictly mediated and controlled user]]. This separation of concerns significantly reduces the overall attack surface, as demonstrated by the security architecture of devices like Apple Vision Pro, which isolates biometric data processing within a dedicated Secure Enclave processor that never exposes raw sensor data to the main OS or applications [105 106]. Trusted Execution Environments (TEEs), such as ARM TrustZone or Intel SGX, can also be leveraged to create secure enclaves for processing highly sensitive data, protecting it even from a compromised operating system [58].

The integration of a "Supervisory Safety Daemon" completes this hardened architecture by introducing a privileged, OS-level process responsible for real-time monitoring and intervention user]]. This daemon operates with higher authority than standard applications and has the mandate to oversee all interactions that affect neuromorphic safety user]]. It continuously monitors for anomalies, threshold breaches, or any activity that violates user-defined neuro-rights policies. For example, if an application attempts to access biometric data without proper consent or initiates an augmented reality effect that could induce motion sickness or seizures, the daemon would detect this violation and intervene [71 93]. Its authority extends to halting, throttling, or revoking access in real time, effectively acting as a final line of defense against malicious or poorly designed applications user]]. This proactive supervision is essential because many XR-specific threats, such as side-channel attacks that infer passwords from head and hand movements [77 78] or perception manipulation techniques that distort a user's sense of reality [93], are difficult to prevent through static security measures alone. The daemon's actions must be transparent to the user, triggering immediate notifications about blocked actions and providing clear pathways for appeal or adjustment of settings user]]. This model combines the strengths of different security paradigms: process isolation contains breaches, formal verification secures the core, and the supervisory daemon provides active, intelligent enforcement. Together, these elements create a resilient security fabric designed to protect the user's neural integrity above all else, fulfilling the core mandate of the Reality.os architecture.

Cross-Platform Interoperability and Compliance Mediation

Achieving broad compatibility across the fragmented AR/VR market is a central pillar of the Reality.os vision, with the OpenXR standard serving as the primary vehicle for universal runtime and device support user]] [11]. OpenXR, developed by the Khronos Group, aims to unify the industry by providing a royalty-free, open standard API that allows developers to build applications that can run across different hardware platforms without relying on proprietary SDKs [13 29]. Nearly all major platforms, including Meta Quest, HTC Vive, Valve SteamVR, Microsoft HoloLens, and PICO, have adopted OpenXR, making it the de facto industry standard for cross-platform development [7 11]. Meta, a founding member and largest contributor to the standard, has publicly shifted its strategy to recommend built-in OpenXR support in popular game engines like Unity and Unreal Engine, recognizing that previous reliance on proprietary plugins created vendor lock-in and undermined the goal of true interoperability [7 8 10]. For Reality.os, this means that a significant portion of the market can be supported through a single, standardized API layer. However, this approach necessitates the creation of rigorous, well-defined cross-platform APIs that act as a secure mediation bridge user]]. These APIs must filter, scrub, and mediate all neuro-data passing between Reality.os and third-party applications, always subject to the user's neuro-rights policies and active consent user]].

The most significant challenge to this OpenXR-centric strategy is the lack of native support for the standard in Apple's VisionOS platform [25 88]. Apple has deliberately chosen to maintain a closed ecosystem, promoting its proprietary suite of frameworks—including ARKit, RealityKit, and PolySpatial—to control the user experience and developer environment [25]. This creates a formidable interoperability barrier, as Reality.os cannot simply rely on a standard OpenXR runtime to function on Vision Pro. To overcome this, the Reality.os architecture must incorporate a dedicated, robust mediation layer specifically designed for Apple's ecosystem. This layer would need to translate Reality.os's internal data structures and security protocols into the formats and calls expected by VisionOS APIs. For instance, it would need to interface directly with ARKit's capabilities for hand tracking, scene reconstruction, world tracking, and object recognition to provide a seamless experience [83]. Crucially, this translation must occur within the tight security constraints of visionOS, which emphasizes on-device processing, minimal data leakage, and user consent for all sensory data access [106]. While workarounds exist, such as treating Vision Pro as an OpenXR-compatible device in Unreal Engine or using specialized Unity packages like XR Hands for VisionOS, these solutions are often unofficial, may not expose all platform features, and require significant additional development effort [85 86 87]. Therefore, a native, deeply integrated adapter module is the most reliable path forward.

This specialized mediation layer for Apple Vision Pro must be architected with security and compliance at its core. It will serve as the critical gatekeeper for all data flows between Reality.os and the Vision Pro environment. Any data crossing this boundary—from biometric inputs like gaze direction and facial expressions to environmental scans of the user's surroundings—must trigger mandatory compliance checks [104 106]. The Reality.os daemon would actively monitor these crossings, ensuring that all access is explicitly permitted by the user's current consent settings and that no neuro-rights policies are violated user]]. For example, if an application attempts to access eye-tracking data to perform emotion recognition, the daemon must block this unless the user has granted specific, informed consent for that particular use case, which falls under the EU AI Act's prohibitions on emotion recognition in certain contexts [42]. Similarly, any attempt to access spatial maps of the user's home or office would be subject to the same stringent approval process, preventing the unauthorized creation of detailed behavioral cartographies [76]. This dual-layered approach—relying on OpenXR for broad compatibility while deploying a specialized, high-assurance mediation layer for Apple's ecosystem—ensures that Reality.os can deliver a consistent, secure, and neuro-rights-compliant experience across the entire spectrum of supported devices.

Real-Time Supervision and Emergency Override Protocols

The "Supervisory Safety Daemon" is the cornerstone of Reality.os's proactive security and ethics enforcement strategy, moving beyond passive logging to active, real-time intervention user]]. This privileged OS-level process is designed to continuously monitor all interactions that could potentially impact neuromorphic safety, such as augmented reality effects, cognitive enhancements, or cross-framework control operations user]]. Its primary function is to act as a guardian of the user's neuro-rights, detecting anomalies or policy violations and responding immediately to mitigate risk. The daemon's authority to halt, throttle, or revoke access in real time is a direct response to the unique dangers posed by immersive technologies, which can manipulate user perception, induce physiological distress, or exploit cognitive vulnerabilities in ways that are impossible in traditional 2D interfaces [71 93]. For example, the daemon would monitor for content that exhibits strobing effects capable of inducing epileptic seizures or perceives user behavior to determine appropriate responses [71]. It would also guard against side-channel attacks, where malicious applications might attempt to infer sensitive information like passwords or PINs from subtle variations in the user's hand and head movements while interacting with a virtual keyboard [77 78].

The enforcement logic of the daemon must be grounded in a formal specification of neuro-rights and safety standards. When a potential violation is detected—for instance, a sudden escalation in the intensity of a neural stimulation protocol or an unauthorized request to share biometric data—the daemon's response must be immediate and decisive. It would first log the event in the secure, tamper-proof consent ledger for later review user]]. Then, it would engage the user with a clear notification explaining the blocked action and the reason for the intervention, prioritizing the user's agency and understanding user]]. Following the notification, it would execute a predefined safety protocol. This could range from temporarily throttling the application's access to sensors to completely halting the operation and revoking its permissions until a new, explicit consent is granted user]]. This real-time feedback loop is critical for empowering users and reinforcing their control over their own cognitive and neural experiences. The effectiveness of this supervision can be enhanced by integrating Runtime Verification (RV) frameworks, which continuously monitor the system's observable behavior against a formal model of correct behavior, automatically flagging deviations that indicate a potential violation or failure [63 66]. RV is particularly well-suited for complex AI-driven systems where full formal verification of the entire system is computationally infeasible, providing a practical way to ensure safety and correctness in the real world [64].

In addition to routine violations, the daemon is responsible for managing severe emergencies through a set of "hard failsafes" designed to prioritize user safety above all else user]]. These emergency protocols are triggered by catastrophic breaches, such as evidence of external manipulation of the system, a breach of a critical safety threshold, or a confirmed cyberattack targeting the device's firmware or software stack. Upon activation, these failsafes would initiate a system lockdown, immediately halting all AR/VR applications and neuromorphic services to prevent further damage or harm user]]. Another emergency response could be a "faint" mode, a low-power state that preserves the device's integrity while disconnecting it from all networks to contain a potential threat user]]. For cross-platform operations that have already been initiated when a violation is detected, the system would trigger a rollback to a known-good state, reverting any changes made during the session to ensure the user's environment and data remain uncompromised user]]. These emergency overrides represent the ultimate expression of the user's right to safety and agency. They are the system's last resort, designed to act autonomously when a situation poses an imminent threat to the user's physical or psychological well-being. By embedding these powerful, user-centric safeguards directly into the OS kernel, Reality.os establishes an unwavering commitment to protecting the user, ensuring that the power of immersive technology is never wielded at the expense of individual safety and dignity.

Policy Alignment and Global Regulatory Integration

The architectural design of Reality.os is not merely a technical exercise; it is a deliberate alignment with a rapidly evolving global consensus on neuro-rights and the ethical governance of neurotechnology. The choice to prioritize Mental Privacy, Cognitive Liberty, Identity Integrity, Agency/Free Will, and Fair Access/Bias reflects a synthesis of recommendations from international bodies, pioneering national legislation, and scholarly discourse [2 3]. The architecture is meticulously crafted to comply with key regulatory frameworks, most notably the European Union's AI Act, which sets a new global benchmark for AI governance [42]. The AI Act's prohibition on AI systems that deploy subliminal or manipulative techniques to distort human behavior directly informs Reality.os's enforcement of Cognitive Liberty [43]. Similarly, its classification of emotion recognition systems as high-risk, with specific prohibitions in workplace and educational settings, reinforces the importance of protecting Mental Privacy [42 71]. By designing the system with real-time overrides and explicit consent requirements, Reality.os preemptively addresses these regulatory demands, positioning itself for compliance as the law takes full effect [43].

The most direct inspiration for Reality.os's neuro-rights framework comes from Chile, which became the first nation to amend its constitution in 2021 to protect mental integrity and regulate the processing of brain activity and its derived information [6 35 101]. Landmark rulings by the Chilean Supreme Court ordering companies like Emotiv to delete collected brain data have established a powerful legal precedent for the enforceability of these rights [18 34 36]. Reality.os's architecture mirrors the spirit of this constitutional protection by placing the user in absolute control of their neural data, a principle that is now influencing legislative efforts in neighboring countries like Mexico, Brazil, and Uruguay [33 36]. Furthermore, the emergence of state-level laws in the United States, such as Colorado's HB24-1058 and California's SB 1223, which classify neural data as sensitive personal information, validates the urgency and necessity of Reality.os's data sovereignty model [6 15 98]. These laws, which require opt-in consent and grant users rights to know, limit disclosure, and delete their data, form the legal bedrock upon which Reality.os's technical controls are built [45].

The table below illustrates the direct mapping between Reality.os's neuro-rights priorities and corresponding international and regional policy instruments, demonstrating a comprehensive and forward-looking approach to governance.

Neuro-Rights Priority	Primary Enforcement Focus in Reality.os	Key International/Regional Policy Instrument(s)
Mental Privacy	Encrypted Vault, Strict API Gating, Consent Ledger	EU GDPR (Art. 9 - Health Data), UNESCO (Ethics of Neurotech), OECD (Responsible Innovation), Chilean Constitution (Art. 19), California SB 1223 [15 16 100 102]
Cognitive Liberty	Real-time Override, Suspension of Manipulative Actions	EU AI Act (Prohibitions on Manipulation), Habeas Cogitationem (Proposed Writ), UN Guiding Principles on Business and Human Rights [40 42 60]
Identity Integrity		

Neuro-Rights Priority	Primary Enforcement Focus in Reality.os	Key International/Regional Policy Instrument(s)
	Biometric Validation, Anti-Spoofing, Session Monitoring	Council of Europe Oviedo Convention, UNESCO Recommendation on the Ethics of Scientific Research [21,60,100]
Agency/ Free Will	Mandatory Explicit Consent, User Override Protocols	Colorado HB24-1058, OECD AI Principles, NIST AI RMF [15,16]
Fair Access & Bias	Algorithm Auditing, Non-Discrimination Protocols, Bias Detection	EU AI Act (High-Risk Systems), UNESCO (Ethics of AI), UN General Assembly Resolution on the Ethics of AI [2,3,43]

By grounding its architecture in these diverse but converging policy frameworks, Reality.os transcends being just a piece of software. It becomes a tangible implementation of a global ethical consensus, offering a blueprint for how technology can be designed to respect and protect fundamental human rights in the age of neurotechnology. This alignment not only mitigates legal and regulatory risk but also builds profound user trust, establishing Reality.os as a leader in responsible innovation.

Compliance Verification and Holistic Risk Management

Ensuring ongoing compliance with its own stringent neuro-rights framework requires a multifaceted and technologically sophisticated verification strategy. Reality.os must move beyond simple periodic audits and instead embed continuous, automated verification into its very fabric. The foundation of this strategy is the use of formal verification for its most critical components, namely the OS kernel and the enforcement modules of the Supervisory Safety Daemon user]]. Formal verification provides a mathematical proof of correctness, guaranteeing that these core elements adhere to their security specifications and cannot be compromised by software bugs or exploits [58,63]. This method offers a level of assurance far superior to traditional testing and is essential for establishing a provably secure foundation upon which all other protections are built. This approach is analogous to the certification processes used for medical devices, where TÜV SÜD and other notified bodies conduct rigorous conformity assessments to ensure cybersecurity and safety [70].

To complement formal verification, Reality.os must implement a continuous monitoring system powered by Runtime Verification (RV) frameworks [63]. While full formal verification of complex, learning-based AI systems is often infeasible, RV provides a practical solution by monitoring the system's observable behavior at runtime against a formal specification [64]. An RV monitor would track key properties related to neuro-rights, such as data access patterns, consent status, and the absence of manipulative behaviors. If the system's behavior deviates from the specification—for example, if an application accesses eye-tracking data after the user has revoked permission—the monitor would flag the violation in real time, triggering an alert and potentially initiating a safety protocol [66]. This creates a dynamic, self-correcting system that can adapt to changing conditions and detect subtle policy violations that might otherwise go unnoticed. The outputs of these monitors can be continuously logged, providing a rich dataset for forensic analysis and improving the models over time, thus enhancing the system's resilience [64].

Finally, no technical system can operate in a vacuum. Reality.os must incorporate robust "human-in-the-loop" oversight to empower users and ensure accountability . This involves providing intuitive, transparent dashboards that visualize data flows, active permissions, and compliance statuses in plain language [46]. Users should be able to easily inspect the secure consent ledger and understand exactly how their data is being used . To combat the erosion of rights through dark patterns, the consent interfaces themselves must be designed according to principles that ensure symmetrical choice, equal effort for all options, and avoidance of emotionally manipulative language [94]. This holistic approach to compliance verification—combining the ironclad guarantees of formal methods, the real-world vigilance of runtime monitoring, and the ultimate authority of human oversight—creates a virtuous cycle of trust and accountability. By proactively addressing the full spectrum of risks, from software vulnerabilities and algorithmic bias to malicious intent and unforeseen emergent behaviors, Reality.os can deliver on its promise of a secure, sovereign, and ethically grounded immersive computing experience.

Reference

1. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM

2. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM

3. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM

4. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?

key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM

5. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM
6. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM
7. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM
8. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.q4m_M0UGtDpbmCGNVQ-k4PKZamO00UWq_bJUsSldHeM
9. OpenXR - High-performance access to AR and VR https://www.khronos.org/openxr/
10. Meta and OpenXR | Meta Horizon OS Developers https://developers.meta.com/horizon/blog/openxr-standard-quest-horizonos-unity-unreal-godot-developer-success/
11. OpenXR https://en.wikipedia.org/wiki/OpenXR
12. OpenXR Boosts Cross-Platform XR as Google's AndroidXR ... https://www.xrtoday.com/mixed-reality/openxr-boosts-cross-platform-xr-as-googles-androidxr-gains-momentum/
13. OpenXR State of the Union https://www.intel.com/content/dam/develop/external/us/en/documents/gdc-2019-khronos-openxr-presentation-807276.pdf
14. Towards new human rights in the age of neuroscience and ... https://pmc.ncbi.nlm.nih.gov/articles/PMC5447561/

15. Regulating neural data processing in the age of BCIs https://pmc.ncbi.nlm.nih.gov/articles/PMC11951885/
16. Mental Privacy and State Responsibility https://constitutionaldiscourse.com/mental-privacy-and-state-responsibility-constitutional-dilemmas-in-the-codification-of-neurorights/
17. Extended Reality (XR) and the Erosion of Anonymity and Pri https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf
18. The protection of neural rights in the age ... https://www.rusjel.ru/jour/article/view/2627?locale=en_US
19. Neurotechnology - Integrating Human Rights in Regulation https://www.geneva-academy.ch/joomlatools-files/docman-files/Neurotechnology%20-%20Integrating%20Human%20Rights%20in%20Regulation.pdf
20. The protection of mental privacy in the area of neuroscience https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf
21. The Regulation of Neuro-Rights* https://www.erdalreview.eu/free-download/979125994752914.pdf
22. Neurorights, Mental Privacy, and Mind Reading | Neuroethics https://link.springer.com/article/10.1007/s12152-024-09568-z
23. Neurotechnologies through the lens of human rights law https://www.techethos.eu/neurotechnologies-through-the-lens-of-human-rights-law/
24. XR packages https://docs.unity3d.com/6000.2/Documentation/Manual/xr-support-packages.html
25. Native visionOS platform support https://news.ycombinator.com/item?id=43768421
26. Create custom environments for your immersive apps in ... https://developer.apple.com/videos/play/wwdc2024/10087/
27. Creating fully immersive experiences in your app https://developer.apple.com/documentation/visionos/creating-fully-immersive-experiences
28. WWDC25: Optimize your custom environments for visionOS https://www.youtube.com/watch?v=RELnRZmb02c
29. Big XR News from Meta, Apple, Microsoft, and OpenXR https://www.xrtoday.com/mixed-reality/big-xr-news-from-meta-apple-microsoft-and-openxr/
30. Getting Started with Apple's Vision OS Development https://blog.learnxr.io/xr-development/getting-started-with-apple-vision-os-development
31. Notes from Apple's “Create immersive media experiences ... https://medium.com/@portemantho/notes-from-apples-create-immersive-media-experiences-for-visionos-8c289e44039e
32. Build immersive web experiences with WebXR - WWDC24 https://developer.apple.com/videos/play/wwdc2024/10066/

33. Privacy and the Rise of “Neurorights” in Latin America https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/

34. Chilean Supreme Court ruling on the protection of brain ... https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2024.1330439/full

35. Neurorights in the Constitution: from neurotechnology to ethics ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11491849/

36. The Controversial Push for New Brain and Neurorights https://www.jmir.org/2025/1/e72270/

37. Chilean Supreme Court ruling on the protection of brain ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10929545/

38. Mind the Gap: Lessons Learned from Neurorights https://www.sciencediplomacy.org/article/2022/mind-gap-lessons-learned-neurorights

39. The Controversial Push for New Brain and Neurorights https://www.sciencedirect.com/org/science/article/pii/S1438887125002808

40. Habeas Cogitationem: A Writ to Enforce the Right ... https://techpolicy.press/habeas-cogitationem-a-writ-to-enforce-the-right-to-freedom-of-thought-in-the-neurotechnological-era

41. What a NeuroRights legislation should not look like https://www.frontiersin.org/journals/neuroscience/articles/10.3389/fnins.2024.1514338/epub

42. Implications of the novel EU AI Act for neurotechnologies https://www.sciencedirect.com/science/article/pii/S089662732400607X

43. High-level summary of the AI Act https://artificialintelligenceact.eu/high-level-summary/

44. Article 6: Classification Rules for High-Risk AI Systems https://artificialintelligenceact.eu/article/6/

45. Neurodata Consent Frameworks: Managing EEG/Brain ... https://secureprivacy.ai/blog/neurodata-consent-eeg-brain-computer-interface-data-gdpr-ccpa

46. European Union Artificial Intelligence Act: a guide https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf

47. NIST PRINCIPLES FOR EXPLAINABLE AI - STIP Compass https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F26746

48. Face biometric recognition with anti-spoofing https://patents.google.com/patent/US20230350996A1

49. Exploring autonomous methods for deepfake detection https://www.sciencedirect.com/science/article/pii/S240584402500653X

50. (PDF) Face Liveness Detection Using Artificial Intelligence ... https://www.researchgate.net/publication/368625224_Face_Liveness_Detection_Using_Artificial_Intelligence_Techniques_A_Systematic_Literature_Review_and_Future_Directions

51. Principles of Designing Robust Remote Face Anti-Spoofing ... https://arxiv.org/html/2406.03684v1

52. FIDO Alliance addresses accuracy and bias in remote ... https://fidoalliance.org/fido-alliance-addresses-accuracy-bias-in-remote-biometric-identity-verification-technologies-industry-first-testing-certification-program/

53. Deepfake Detection — Reality Defender https://www.realitydefender.com/

54. Liveness detection - Security for anti-spoofing - Fraud.com https://www.fraud.com/post/liveness-detection

55. Enhanced secure storage and data privacy management ... https://www.nature.com/articles/s41598-025-16624-y

56. Privacy preservation in Artificial Intelligence and Extended ... https://www.sciencedirect.com/science/article/pii/S1084804524001668

57. A Developer-Centered Study of Security and Privacy ... https://arxiv.org/html/2509.06368v1

58. Chapter 0 Innovating Augmented Reality Security https://arxiv.org/html/2509.10313v1

59. Brain Computer Interfaces and Human Rights: Brave new ... https://dl.acm.org/doi/fullHtml/10.1145/3531146.3533176

60. Perspective Chapter: Making Space for Neuro Rights in the ... https://www.intechopen.com/chapters/88036

61. On Neurorights https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2021.701258/full

62. Making Space for Neuro Rights in the Context of Brain ... https://www.researchgate.net/publication/377201427_Perspective_Chapter_Making_Space_for_Neuro_Rights_in_the_Context_of_Brain-Computer_Interfaces_One_Small_Step_for_Human_Rights_One_Giant_Leap_for_Mankind

63. Verification for Machine Learning, Autonomy, and Neural ... https://arxiv.org/pdf/1810.01989

64. Runtime Verification for Deep Learning Systems https://www.scitepress.org/Papers/2025/131955/131955.pdf

65. Case Study: Runtime Safety Verification of Neural Network ... https://dl.acm.org/doi/10.1007/978-3-031-74234-7_13

66. Runtime Verified Neural Networks for Cyber-Physical ... https://dl.acm.org/doi/10.1145/3679008.3685547

67. Verification for Machine Learning, Autonomy, and Neural ... https://www.researchgate.net/publication/328091692_Verification_for_Machine_Learning_Autonomy_and_Neural_Networks_Survey

68. Verification for Machine Learning, Autonomy, and Neural ... https://www.semanticscholar.org/paper/95588f6f59e9e0175a5d3266506626ac063ef666

69. Neural personal information and its legal protection: evidence ... https://academic.oup.com/jlb/article/12/1/lsaf006/8113730

70. Neurological device testing and certification https://www.tuvsud.com/en/industries/medical-devices/neuro

71. Safety and Privacy in Immersive Extended Reality https://link.springer.com/article/10.1007/s44206-024-00114-1

72. Enforcement Design Patterns in EU Law: An Analysis of the ... https://link.springer.com/article/10.1007/s44206-024-00129-8

73. REALITY Privacy Policy (Android) https://reality.app/legal/privacy_policy_android_en.html

74. Neural Networks API - NDK https://developer.android.com/ndk/guides/neuralnetworks

75. Android XR: Building the Next Reality. https://blogs.infosys.com/emerging-technology-solutions/artificial-intelligence/android-xr-building-the-next-reality.html

76. Top XR Security Risks Every Business Should Know https://www.xrtoday.com/mixed-reality/top-xr-security-risks-every-business-should-know/

77. Taxonomy and Analysis of Security Vulnerabilities, Privacy ... https://dl.acm.org/doi/10.1145/3733155.3733199

78. Security and privacy in virtual reality: a literature survey https://link.springer.com/article/10.1007/s10055-024-01079-9

79. XR Security Compliance Case Studies: How Regulated ... https://www.xrtoday.com/mixed-reality/xr-security-compliance-case-studies-how-regulated-industries-secure-xr-environments/

80. A Cybersecurity Risk Assessment for Enhanced Security in ... https://www.mdpi.com/2078-2489/16/6/430

81. Machine learning – based perspectives on risk, trust, and ... https://www.sciencedirect.com/science/article/pii/S2667096825000382

82. OpenXRLab XRAPI is an open-source implementation of ... https://github.com/openxrlab/xrapi

83. ARKit in visionOS | Apple Developer Documentation https://developer.apple.com/documentation/arkit/arkit-in-visionos

84. Manual: PolySpatial visionOS https://docs.unity3d.com/Manual/com.unity.polyspatial.visionos.html

85. Cross Platform Porting to the Vision Pro with Unity https://medium.com/@dariony/cross-platform-porting-to-the-vision-pro-with-unity-59bfb30b54df

86. Hands input for Fully Immersive VR - OpenXR or VisionOS? https://discussions.unity.com/t/hands-input-for-fully-immersive-vr-openxr-or-visionos/333324

87. #1481: Agile Lens 2024: Context on Boz's Apology to ... https://voicesofvr.com/1481-agile-lens-2024-context-on-bozs-apology-to-vr-devs-orion-ar-glasses-impressions-unreal-engine-mediation-with-apple-meta/
88. Apple Vision Pro First Impressions with Road to VR's Ben ... https://voicesofvr.com/1346-apple-vision-pro-first-impressions-with-road-to-vrs-ben-lang-the-comparisons-to-meta-quest/
89. Implications of XR on Privacy, Security and Behaviour http://www.mkhamis.com/data/papers/abraham2022nordichi.pdf
90. Recent Trends of Authentication Methods in Extended Reality https://www.mdpi.com/2571-5577/7/3/45
91. Privacy-Preserving Brain-Computer Interfaces https://arxiv.org/html/2412.11394v1
92. Privacy-Preserving Brain − Computer Interfaces https://www.researchgate.net/publication/367672143_Privacy-Preserving_Brain-Computer_Interfaces_A_Systematic_Review
93. A Systematic Analysis of Deceptive Design in Extended ... https://dl.acm.org/doi/10.1145/3659945
94. Dark Patterns as Disloyal Design https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11577&context=ilj
95. Cybersecurity and Privacy Challenges in Extended Reality https://www.mdpi.com/2813-2084/4/1/1
96. (PDF) A Review of Security and Privacy Challenges in ... https://www.researchgate.net/publication/387061820_A_Review_of_Security_and_Privacy_Challenges_in_Augmented_Reality_and_Virtual_Reality_Systems_with_Current_Solutions_and_Future_Directions
97. Safeguarding Brain Data: Assessing the Privacy Practices ... https://perseus-strategies.com/wp-content/uploads/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf
98. Examining the New Frontier of Brainwaves and Data Privacy https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1507&context=ncjolt
99. The ethical and legal landscape of brain data governance - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC9799320/
100. To the edge of data protection: How brain information can ... http://arno.uvt.nl/show.cgi?fid=145874
101. Brain Data in Context: Are New Rights the Way to Mental ... https://www.researchgate.net/publication/369824294_Brain_Data_in_Context_Are_New_Rights_the_Way_to_Mental_and_Brain_Privacy
102. MACHINE INTERFACES https://www.albanylawscitech.org/api/v1/articles/19163-inside-the-mind-s-eye-an-international-perspective-on-data-privacy-law-in-the-age-of-brain-machine-interfaces.pdf

103. Your Data is Secure | Meta Quest https://www.youtube.com/watch?v=lilPCP_R-bg

104. Meta Quest Pro | Privacy & security guide https://www.mozillafoundation.org/en/privacynotincluded/meta-quest-pro/

105. Apple Vision Pro - Technical Specifications https://www.apple.com/apple-vision-pro/specs/

106. Apple Vision Pro Privacy Overview https://www.apple.com/privacy/docs/Apple_Vision_Pro_Privacy_Overview.pdf

107. Hardware backed integrity and runtime attestation https://learn.microsoft.com/en-us/hololens/security-hardware-backed-integrity

108. Security overview - HoloLens https://learn.microsoft.com/en-us/hololens/security-overview

109. HoloLens 2 Security FAQ https://www.spheregen.com/hololens-2-security-faq/