Qwen

From Shard to Sovereign: A Blueprint for Governance-Aware Neuromorphic Architectures

Abstract Governance Patterns Derived from Sharding Principles

The development of a governance-aware neuromorphic architecture necessitates a fundamental reconceptualization of sharding. Traditionally, sharding is framed as a technical strategy for enhancing raw performance through benefits like memory savings, scalability, faster inference, higher throughput, and improved reliability . This research framework inverts this paradigm, treating these same features not as levers for maximizing model power but as foundational systems constraints that enable safe, sovereign, and ecologically responsible intelligence . By reframing sharding's capabilities as enforceable architectural principles, a robust set of abstract, transferable governance patterns emerges. These patterns are designed to be jurisdiction-agnostic, providing a flexible yet principled substrate upon which specific regulatory requirements can later be layered. The core insight is that sharding becomes a mechanism for embedding sovereignty directly into the computational fabric, ensuring that any gain in efficiency is purposefully allocated to compliance, safety, and social good rather than unbounded growth.

A primary pattern derived from this reframing is **Surplus Allocation for Ecological and Social Good**. The efficiency gains achieved through sharding—whether in memory, compute, or energy—must be formally designated to serve purposes beyond the immediate operation of the neuromorphic model . For instance, a fixed percentage of the saved resources, perhaps between 20% and 30%, could be programmatically allocated to environmental and social objectives . This could include running continuous live energy metering to track operational carbon footprint, enabling carbon-aware job scheduling where computationally intensive tasks are deferred during periods of high renewable energy availability, deploying anomaly detection models to identify misuse or malicious activity, and participating in federated ecological modeling initiatives [2] [8] . This pattern operationalizes the ESG (Environment, Social, Governance) framework for sustainable AI by making commitments to environmental stewardship and social benefit a direct

engineering mandate, not an optional add-on [2]. It transforms the theoretical promise of green AI into a concrete architectural requirement, directly linking hardware efficiency to tangible societal contributions.

Another critical pattern is **Multi-Signature Approval for Systemic Changes**. The ability to scale a distributed system, for example by adding new shards or increasing parameter counts, represents a significant escalation of power. To prevent unilateral or predatory scaling, any such topology-altering change must require multi-signature approval from distinct, pre-defined stakeholder groups . This mirrors established practices in decentralized finance and blockchain governance, where no single entity has unchecked authority [14]. In this context, a transaction to re-shard or deploy a larger model would require cryptographic signatures from at least one representative each from the technical lead, the legal/compliance department, and an independent ethics or ecology steward . This creates a formalized check-and-balance mechanism, ensuring that escalations of system capability are subject to collective oversight and deliberation before implementation. This pattern fundamentally decouples the technical capacity for scaling from the decision-making authority over it, introducing a crucial layer of governance that prevents rapid, uncoordinated, and potentially irresponsible growth.

The third abstract pattern is **Co-Evolution with Human Institutions**. As neuromorphic systems evolve, their complexity and influence increase. This pattern mandates that any planned increase in model size or context length must be accompanied by a rigorous, documented process demonstrating its continued compatibility with existing human-centric governance frameworks, such as ALN (Augmented Legal Identity), KYC (Know Your Customer), and DID (Decentralized Identifier) systems . Furthermore, every significant system update must be paired with updated public documentation detailing the changes and their potential impacts . This makes the system's evolutionary path auditable, transparent, and accountable to its human stakeholders. It ensures that technological advancement does not outpace the development of the legal, ethical, and social structures needed to manage it responsibly. This principle fosters a relationship of trust between the system and its users, grounded in transparency and a demonstrated commitment to co-evolution rather than autonomous, opaque progression.

Finally, the concept of **Jurisdictional Segmentation via Shard Partitioning** provides a powerful mechanism for enforcing data sovereignty at the architectural level. Instead of treating the neuromorphic network as a monolithic entity, it can be partitioned into legally-scoped "cognitive regions," where individual shards or groups of shards are physically and logically constrained to operate within the boundaries of specific jurisdictions . Data originating from the European Union, for example, would be processed exclusively on EU-bound shards, thereby satisfying stringent data-residency

and sovereignty requirements without relying solely on complex contractual agreements or post-hoc data transfers [15] [18]. Each shard would carry a machine-readable "legal profile" corresponding to the regulations of its assigned region, which is enforced through compile-time and run-time checks . This approach converts the challenge of cross-border compliance into a manageable infrastructure design problem, allowing the system to be inherently portable while still permitting precise bindings to local laws where necessary [20]. This pattern effectively builds sovereignty directly into the system's topology, ensuring that data processing is always aligned with the legal and cultural norms of the citizenry it serves.

Concrete Benchmarks for Non-Predatory Performance and Ecological Responsibility

To transition the abstract governance patterns from conceptual ideals to practical, verifiable standards, a comprehensive set of concrete metrics and benchmarks must be established. These benchmarks form the quantitative backbone of a non-predatory neuromorphic architecture, providing measurable criteria against which performance, safety, and ecological impact can be assessed. The focus shifts from chasing raw throughput or model size to optimizing for a balanced scorecard of efficiency, fairness, accountability, and well-being. These metrics are essential for creating an auditable and trustworthy system that operates within predefined ethical and environmental envelopes.

A cornerstone metric is the **Energy-per-Inference Ceiling**. Spiking Neural Networks (SNNs), a key type of neuromorphic architecture, are inherently low-power due to their event-driven nature, activating only when significant events occur [3]. This offers a substantial energy advantage over conventional Artificial Neural Networks (ANNs) that use continuous-valued representations [3]. For example, one SNN deployed on Intel's Loihi chip achieved a 110-fold reduction in energy per inference compared to traditional methods [8]. The research framework must formalize these gains by establishing a hard ceiling on the maximum allowable energy consumption for any given inference task, measured in millijoules (mJ) or joules (J) per inference [2] [8]. This metric directly ties the hardware's intrinsic efficiency to a non-predatory operational constraint, ensuring that the system's pursuit of intelligence remains cognizant of its environmental cost. Any model deployment or inference request that exceeds this ceiling would trigger a system response, such as being deprioritized, downgraded in complexity, or routed to a more energy-efficient shard.

To address the "black box" problem inherent in complex AI models, a suite of metrics focused on **Audit Completeness and Traceability** is required. Blockchain technology presents a compelling solution for creating transparent, immutable, and verifiable audit trails [4]. A "Traceability Score" can be developed based on a formal framework of auditability axioms, such as those proposed for characteristically auditable multi-agent systems: Integrity (tamper-proof entries), Coverage (all relevant events are recorded), Temporal Coherence (causal ordering is preserved), Verifiability (entries can be independently verified), Accessibility (authorized parties can retrieve logs), Resource Proportionality (overhead scales reasonably), Privacy Compatibility (complies with privacy laws), and Governance Alignment (supports external regulations) [6]. Every significant system event—from shard creation and model updates to user queries and actuator commands—would be recorded as a transaction on a dedicated blockchain ledger [4]. The Traceability Score would then quantify how rigorously the system adheres to these eight axioms, providing a real-time assessment of its auditability. Case studies in financial services, healthcare, and public sector applications have shown that blockchain auditing can improve user trust, reduce liability insurance premiums, and ensure greater transparency in algorithmic decision-making [4].

For augmented citizens, fairness must be quantified and tied to their status within the system. This leads to the definition of **Fairness and Non-Exploitation Indices**. A "Fairness Index" could be calculated by analyzing the distribution of system resources, such as latency and throughput, among authenticated identities. This index would ensure that the system's increased capacity is used to provide fair access to a larger number of users, rather than amplifying the power available to a single actor . The index could flag disproportionate resource allocation and trigger corrective measures. Complementing this is a "Non-Exploitation Score," which leverages privacy-preserving technologies like Differential Privacy (DP) [13] [14]. DP adds calibrated statistical noise to data or model gradients to prevent the re-identification of individuals, thus protecting them from exploitation through data mining [13]. The Non-Exploitation Score would measure the effectiveness of these privacy mechanisms, for example, by tracking the privacy budget (ε) used in DP implementations and correlating it with the accuracy of the resulting model [14]. This provides a concrete measure of how well the system protects individual privacy during its operations.

Perhaps most critically for human-augmented systems, the framework must introduce metrics for **Bioload and Biostretched-Zone Risk Bands**. "Bioload" refers to the cumulative cognitive and physiological stress imposed on a human user by interacting with the neuromorphic system. This requires defining measurable risk bands (e.g., low, medium, high) based on real-time inputs from biometric sensors monitoring signals like

EEG, heart rate variability, or galvanic skin response [10]. These bands would be tied to specific thresholds of cognitive load or physiological arousal. When a user's bioload enters a "high" risk band, it triggers predefined **Biostretched-Zone Policies**. These policies represent a direct link between the user's biological state and the system's operational parameters. For example, a high-risk entry might automatically initiate "tissue-safe duty cycling," which involves pausing non-critical computations or reducing the system's responsiveness to give the user's nervous system time to recover . Another policy could involve forcing the user's interface into a lower-power mode, akin to what might be termed "Reality.os bioload scheduling," to reduce sensory input and cognitive demand . This integration of biological feedback loops into the control system represents a profound shift towards a user-centric architecture where the well-being of the augmented citizen is a first-order constraint on all computational activities.

Metric Category	Specific Metric/ Benchmark	Description	Governing Principle
Ecological Responsibility	Energy-per-Inference Ceiling	A hard limit on the maximum energy (in mJ or J) consumed per inference task, enforced as a system-wide constraint [8].	Sustainability & Environmental Stewardship
Accountability	Audit Completeness & Traceability Score	A quantitative measure of adherence to auditability axioms (Integrity, Coverage, etc.) based on records in an immutable blockchain ledger [4] [6].	Transparency & Verifiability
Social Equity	Fairness & Non-Exploitation Index	A composite score measuring equitable resource distribution among authenticated users and the effectiveness of privacy-preserving techniques like Differential Privacy [13] [14].	Equitable Access & Privacy Protection
Human Safety	Bioload & Biostretched-Zone Risk Bands	Thresholds for cognitive/physiological stress levels, triggering automated safety protocols like tissue-safe duty cycling or reduced system responsiveness .	Cognitive Liberty & Mental Integrity

Regulatory Profile Integration and Cross-Jurisdictional Compliance

A truly sovereign neuromorphic architecture must navigate a complex and fragmented global landscape of data protection and neurotechnology regulation. The proposed framework addresses this challenge through a two-tiered approach: a foundation of abstract, jurisdiction-agnostic governance patterns, which serve as a flexible substrate, and a dynamic overlay of specific regulatory "profiles" tailored to the laws of different jurisdictions . This modular design allows the core architecture to remain portable and adaptable, capable of seamlessly attaching the appropriate legal and ethical guardrails based on the context of the data being processed or the identity of the citizen interacting

with the system. This method ensures that the system can operate globally while respecting the unique legal traditions and societal values of each region.

The first tier of this approach consists of the abstract governance patterns previously discussed, such as Surplus Allocation, Multi-Signature Approval, and Jurisdictional Segmentation . These patterns create a robust default configuration for the system. They establish a baseline of safety, fairness, and ecological responsibility that applies universally. The second tier involves mapping specific legal regimes onto this foundation. For example, a shard processing data from the European Union would automatically attach a "GDPR & Neurorights Profile." This profile would translate the abstract pattern of "strong data protection" into concrete, executable rules. It would mandate adherence to GDPR's strict consent requirements for sensitive data categories, which already encompass biometric information [15]. More significantly, it would incorporate principles from emerging neurorights charters, such as Chile's proposed legislation, which equates brain data with organ donation and establishes absolute prohibitions against unauthorized intrusions into mental processes [9] [11]. This profile would configure the shard to treat neuronal data as the most sensitive category of personal information, preventing its sale or transfer and requiring explicit, informed consent for any processing [9] [17].

Similarly, a shard operating within the United States would need to accommodate a patchwork of federal and state laws. A "HIPAA Profile" would be essential for any shard handling data related to medical diagnoses or treatments, mandating strict controls on Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act [18] [20]. Meanwhile, a "California SB 1223 / Colorado CPA Profile" would become active when the system interacts with residents of those states. These laws explicitly define "neural data" and regulate its collection and use, particularly in contexts like neuromarketing [19] [20]. The associated profile would enforce requirements for clear disclosure to consumers when neuromarketing tools are used and mandate obtaining explicit opt-in consent before collecting any biometric or neurological data [19]. It would also restrict marketing targeted at vulnerable populations like children and the elderly [19]. This demonstrates how the abstract pattern of "human-centered consent" is concretely implemented to protect consumers from novel forms of manipulation.

Furthermore, emerging high-level regulations like the European Union's AI Act introduce a new dimension of compliance through risk classification. An "AI Risk Classification Profile" can be attached to shards based on the intended application of the neuromorphic system. The EU AI Act, for instance, classifies certain applications, such as emotion recognition systems used in workplace or educational settings, as "high-risk" and places

severe restrictions on their use [20]. A shard performing such a function would automatically activate this profile, which would trigger a cascade of additional safeguards. These could include mandatory human-in-the-loop supervision, enhanced logging and reporting, and stricter validation procedures to ensure the system does not infringe on fundamental rights like freedom of thought or mental integrity [12] [20]. This risk-based approach allows the system's governance posture to dynamically adapt to the specific societal risks posed by its own functionality.

The following table illustrates how abstract governance patterns can be mapped to specific regulatory profiles, demonstrating the flexibility and power of the proposed framework.

Abstract Governance Pattern	GDPR & Neurorights Profile Example	US HIPAA Profile Example	California SB 1223 Profile Example	EU AI Act "High-Risk" Profile Example
Strong Data Protection	Classify all brain data as special category/sensitive health data under Article 9 of GDPR; mandate explicit, granular consent; prohibit data sales [15] [17].	Enforce strict rules for Protected Health Information (PHI); require Business Associate Agreements (BAAs) with all data handlers [18] [20].	Mandate clear consumer disclosure before neural data collection; require explicit opt-in consent for all uses [19].	Trigger enhanced logging, human oversight, and bias monitoring requirements; prohibit use cases that pose an unacceptable risk to rights [20].
Human-Centered Consent	Implement Dynamic Consent (DC) frameworks allowing users to grant/revoke consent for specific data uses in real-time [20].	Ensure patient consent for data use aligns with HIPAA's minimum necessary standard and authorization requirements [20].	Require interactive consent dashboards where users can understand and control how their neural data is used [19].	Enforce that meaningful human oversight is maintained, especially for high-stakes decisions, to prevent algorithmic determinism [20].
Transparency & Explainability	Adhere to GDPR's right to explanation for automated decisions; provide clear information on how algorithms using brain data function [15].	Comply with transparency requirements for covered entities regarding privacy practices and data use [20].	Mandate standardized disclosure formats explaining neuromarketing techniques and data usage to consumers [19].	Require detailed technical documentation and public summaries of the AI system's capabilities, limitations, and risk mitigation measures [20].
Safety & Wellbeing	Incorporate the Chilean neuroright to mental integrity, implementing technical safeguards to detect and block unauthorized brain data alteration [9].	Follow FDA guidelines for medical device safety and effectiveness, including risk management and post-market surveillance [17].	Restrict marketing using neural data from targeting vulnerable groups (e.g., children, cognitively impaired) [19].	Mandate systematic examination of subjective effects and potential for self-alienation, with provisions for psychological support [12].

This profile-based architecture enables the neuromorphic system to function as a compliant entity in multiple jurisdictions simultaneously. For instance, a multinational corporation could operate a single, globally distributed neuromorphic network, with each shard configured according to the legal profile of the country in which it resides and processes data. This approach avoids the inefficiency and legal ambiguity of attempting

to apply a single, monolithic set of rules to a diverse global user base, instead embracing regulatory pluralism as a core feature of its design.

Infrastructure-Governance Co-Specification for Human Augmentation

The most innovative and challenging aspect of developing a governance-aware neuromorphic architecture is the explicit, bidirectional integration of infrastructure design with human-augmentation governance. This requires moving beyond a purely top-down regulatory model and instead co-specifying the system's physical and logical components—its shards, schedulers, and topology—with the rights, safety, and well-being of the augmented citizen. Every infrastructure decision must have a direct line to human-centric conditions, ensuring that the system's operation is fundamentally accountable to the people it is designed to augment. This tight coupling transforms abstract rights and safety principles into concrete, enforceable technical specifications.

This co-specification begins with **Shard Partitioning as the Basis for Augmented-Citizen Rights**. The jurisdictional and governance profile of a shard directly defines the legal landscape and rights available to a citizen interacting with it. This enables the concept of **Dynamic Autorights Expansion**, where a user's rights are not static but can expand or contract based on their interaction context. For example, a citizen in the United States interacting with a shard governed by a "Chilean Neurorights Profile" (perhaps because they are accessing a service hosted in Chile) might temporarily acquire a higher baseline of rights, such as stronger protections for data deletion or a heightened right to mental privacy [9]. Conversely, if the same citizen connects to a less regulated shard, their rights might be scaled back accordingly. The infrastructure partitioning itself becomes the mechanism for delivering this variable rights framework. The system's identity management layer (ALN/KYC/DID) would not only authenticate the user but also dynamically map their identity to the appropriate rights schema based on the shard's location and profile, creating a fluid and context-aware rights environment.

The system scheduler plays a crucial role in this integrated model, acting as the executive arm of human safety protocols. It must be co-designed with **Tissue-Safe Duty Cycling** mechanisms. The scheduler cannot operate in a vacuum, prioritizing tasks based solely on computational urgency. Instead, it must receive and act upon real-time biological feedback from the user's augmentations . If a user's EEG or other biometric sensors indicate signs of excessive cognitive load or physiological stress, signaling an entry into a

"biostretched-zone," the scheduler's behavior must change. It could preemptively offload computationally intensive tasks to another shard, reduce the complexity or verbosity of system-generated responses, or place the user's interface into a lower-power, less stimulating mode . This "tissue-safe duty cycling" ensures that the system's computational demands never exceed the physiological tolerance of the human host, making the user's well-being a primary constraint on system performance.

Furthermore, major infrastructure changes must be subject to human governance review. The process of updating the system's topology—for example, re-sharding to rebalance load or deploying a new model version—should not be an automated, algorithmic process. Instead, it must engage **Neuroscore-Adept Panels** . These panels would consist of interdisciplinary experts, including neuroscientists, ethicists, and technologists, who are responsible for interpreting the system's performance metrics. A "Neuroscore" could be a composite metric reflecting various aspects of system and user interaction quality, such as cognitive load, emotional valence, and task completion success. Before a major change is implemented, the panel would review the projected Neuroscores and assess the potential impact on user safety and cognitive integrity. Their approval would be a prerequisite for the change, providing a vital human-in-the-loop check on purely optimization-driven decisions. This ensures that infrastructure evolution is guided not just by efficiency but also by a deep consideration of its human consequences.

Finally, this co-specification extends to the very consensus mechanisms used by the neuromorphic network. A Proof-of-Spiking-Neurons (PoSN) protocol, for example, offers a fascinating model for distributed self-governance [1] . In PoSN, transactions are encoded as spike trains, and leader election is determined by the earliest spiking neuron, which could represent a shard or node [1] . The probability of a shard being elected leader could be weighted by a "stake" variable. This stake could be a composite of factors, including the shard's jurisdictional importance, its contribution to ecological goals (as measured by its surplus allocation), and the aggregate Neuroscores of its users. This creates a system where governance is not imposed from a central authority but emerges from the distributed network, with each shard's voting power proportional to its contribution to the overall system's sovereignty, sustainability, and well-being. Such a protocol embodies the principle of distributed self-governance, where shards negotiate or vote before taking system-level actions, with each shard weighted by its jurisdictional and ecological "stake" .

Infrastructure Component	Human-Augmentation Governance Mechanism	Technical Specification
Shard Partitioning	Dynamic Autorights Expansion	The shard's legal profile (e.g., GDPR, Chilean Neurorights) is used to instantiate a specific rights schema for the connected user's ALN identity.
System Scheduler	Tissue-Safe Duty Cycling	The scheduler receives real-time biometric data (EEG, HRV) and adjusts task prioritization, complexity, or responsiveness to keep user bioload within safe risk bands .
Topology Management	Neuroscore-Adept Panel Review	Major system changes (e.g., re-sharding, model updates) require cryptographic approval from a human expert panel whose judgment is based on predictive Neuroscore analysis .
Consensus Protocol	Distributed Self-Governance	Leader election or voting weight is determined by a stake variable incorporating jurisdictional significance, ecological contribution, and user Neuroscore metrics [1] .

By designing the infrastructure with these human-augmentation mechanisms as first-class citizens, the neuromorphic architecture ceases to be a mere tool and becomes a partner in augmenting human potential, one that is bound by the same principles of safety, fairness, and respect for personhood that govern our society.

Synthesis: An Integrated Model for Safe and Sovereign Intelligence

This research report has outlined a comprehensive framework for developing governance-aware neuromorphic architectures, shifting the paradigm of sharding from a tool for raw performance maximization to an enabler of safe, sovereign, and ecologically responsible intelligence. The proposed model is built upon a multi-layered structure that integrates abstract, jurisdiction-agnostic governance patterns with concrete, measurable benchmarks for non-predatory performance, and explicitly links infrastructure design to the rights and safety of augmented humans. This synthesis culminates in an integrated model where sovereignty is not an external compliance layer but an intrinsic property of the system's computational fabric.

The foundation of this model is the reframing of sharding's benefits as enforceable constraints. Memory savings are not used to build larger, more opaque models, but are reserved for a dedicated "safety budget" for monitoring and compliance modules . Scalability is channeled into a "bounded scaling policy" that operates within pre-approved legal and ethical envelopes, enforced by multi-signature approvals that prevent unilateral escalation . Latency gains are allocated for "latency for oversight," embedding safety filters directly into the operational workflow before any output is released . Throughput

is managed through "rate-limited, identity-aware access" to ensure fair service for all, not just amplified power for a few . And reliability is enhanced through "fault-tolerant ethics," where every shard carries replicated minimal safety logic to ensure the system fails closed in the event of a failure . These principles transform sharding from a purely technical optimization into a foundational pattern for sovereignty-first infrastructure.

This architectural foundation is then made actionable through a set of concrete, quantifiable metrics. **Energy-per-inference ceilings** enforce ecological responsibility, turning the inherent efficiency of neuromorphic hardware into a verifiable commitment to sustainability [2] [8] . **Audit completeness and traceability scores**, anchored in immutable blockchain ledgers, combat the "black box" problem and provide a rigorous measure of system transparency and accountability [4] [6] . **Fairness and non-exploitation indices** ensure that the system's power is distributed equitably and that privacy is protected through mechanisms like differential privacy [13] [14] . Most critically, the introduction of **bioload and biostretched-zone risk bands**, along with associated tissue-safe duty cycling policies, creates a direct feedback loop between the user's biological state and the system's operational parameters, making the well-being of the augmented citizen a primary design constraint .

The system's portability and adaptability are achieved through a modular regulatory profile system. Abstract patterns like strong data protection and human-centered consent serve as a universal baseline, which can be dynamically augmented with specific legal "profiles" tailored to jurisdictions like the EU (GDPR), the US (HIPAA, CCPA), or emerging international standards (EU AI Act) [15] [19] [20] . This allows a single, globally distributed architecture to comply with diverse legal regimes simultaneously, respecting the unique societal values of each region.

Ultimately, the framework's most profound contribution is its explicit co-specification of infrastructure and human-augmentation governance. Shard partitioning becomes the mechanism for delivering dynamic autorights expansions . The system scheduler is tasked with implementing tissue-safe duty cycling based on real-time biometric feedback . And major infrastructure changes are subject to review by neuroscore-adept panels, ensuring that evolution is guided by human judgment . This tight coupling ensures that every technical decision is imbued with a sense of responsibility to the human user, reconceptualizing the neuromorphic system not as a disembodied intelligence, but as an integral part of an augmented human ecosystem.

While challenges remain, including the need for standardized software APIs, careful management of embodied carbon footprints, and the further development of human-computer interaction paradigms for concepts like "Reality.os," this framework provides a

clear and actionable blueprint. It moves the field of neuromorphic computing toward a future where intelligence is not merely powerful, but also safe, sovereign, and deeply respectful of the humans it is designed to serve.

Reference

1. Proof-of-Spiking-Neurons(PoSN): Neuromorphic Consensus for ... https://arxiv.org/html/2511.02868v1
2. Neuromorphic hardware for sustainable AI data centers This ... - arXiv https://arxiv.org/html/2402.02521v2
3. The Promise of Spiking Neural Networks for Ubiquitous Computing https://arxiv.org/html/2506.01737v1
4. Using Blockchain to Audit AI Model Decisions - LinkedIn https://www.linkedin.com/pulse/using-blockchain-audit-ai-model-decisions-andre-gkfge
5. Bio-Rollup: a new privacy protection solution for biometrics based ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11419648/
6. Creating Characteristically Auditable Agentic AI Systems - ACM https://dl.acm.org/doi/10.1145/3759355.3759356
7. A privacy-preserving scheme with multi-level regulation compliance ... https://www.nature.com/articles/s41598-023-50209-x
8. [PDF] The Promise of Spiking Neural Networks for Ubiquitous Computing https://arxiv.org/pdf/2506.01737
9. What Should We Do With People Who Cannot or Do Not Want to Be ... https://pmc.ncbi.nlm.nih.gov/articles/PMC8371680/
10. 'Neurorights' (Chapter 24) - The Cambridge Handbook of ... https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/neurorights/AF85DE57D51D114E26C19146E234F897
11. Neurorights – Do we Need New Human Rights? A Reconsideration ... https://link.springer.com/article/10.1007/s12152-022-09511-0
12. Full article: What an International Declaration on Neurotechnologies ... https://www.tandfonline.com/doi/full/10.1080/21507740.2023.2270512
13. A service-oriented microservice framework for differential privacy ... https://pmc.ncbi.nlm.nih.gov/articles/PMC12335493/

14. Exploring privacy mechanisms and metrics in federated learning https://link.springer.com/article/10.1007/s10462-025-11170-5
15. Neurotechnology Governance in the United States - PMC - NIH https://pmc.ncbi.nlm.nih.gov/articles/PMC12797108/
16. [PDF] framework for anticipatory governance of emerging technologies https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/framework-for-anticipatory-governance-of-emerging-technologies_14bf0402/0248ead5-en.pdf
17. Towards a Governance Framework for Brain Data | Neuroethics https://link.springer.com/article/10.1007/s12152-022-09498-8
18. International Data Governance for Neuroscience - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC8857067/
19. Regulating the Mind: Neuromarketing, Neural Data and Stakeholder ... https://www.mdpi.com/2076-3387/15/10/386
20. Regulating neural data processing in the age of BCIs: Ethical ... https://journals.sagepub.com/doi/abs/10.1177/20552076251326123