A Foundational Report on Neural Rights: Protecting Cognitive Liberty and Mental Integrity in the Age of Neurotechnology

Defining the New Frontier: The Emergence and Core Principles of Neural Rights

The concept of Neural Rights represents a paradigm shift in human rights discourse, emerging as a direct response to the profound ethical, legal, and social challenges posed by the rapid advancement of neurotechnology [4 72]. These rights are not merely an extension of existing legal principles but a new category of fundamental entitlements designed to safeguard the uniquely intimate domain of the human brain and mind from unauthorized access, manipulation, and exploitation [101]. The genesis of this movement can be traced to the early 21st century, with foundational work by scholars such as Marcello Ienca and Roberto Andorno who formally articulated four core neuro-specific rights in 2017: cognitive liberty, mental privacy, mental integrity, and psychological continuity [4 101]. Their proposal argued that traditional human rights frameworks were insufficient to address the novel threats posed by technologies capable of reading and writing neural information [3 7]. Dr. Rafael Yuste, a leading advocate and Professor at Columbia University, further propelled this agenda by warning that neurotechnologies could now decode or manipulate human thoughts, creating unprecedented challenges for established human rights instruments [6]. The Morningside Group, a collective of scientists and lawyers led by Yuste, published a pivotal paper in 2017 using a hypothetical BCI-related crime to highlight how existing laws failed to adequately protect agency and freedom of thought [7 9].

The core principles of Neural Rights have since coalesced around five universally recognized pillars, which provide a comprehensive framework for protecting cognitive liberty and mental integrity. The first and most foundational principle is Mental Privacy, the right to keep one's thoughts, neural patterns, and mental states private from unauthorized collection, surveillance, or use [6 72]. This principle recognizes that neural data is fundamentally different from other biometric identifiers; it is not just a marker of identity but a direct window into an individual's consciousness, revealing subconscious processes, emotions, and intentions [40 78]. The Chilean Supreme Court's landmark ruling against Emotiv Inc. underscored this by rejecting the company's claim that pseudonymized EEG data was not personally identifiable, emphasizing that neurodata represents the most intimate aspects of human personality [78]. The second pillar is Cognitive Liberty and Agency, which encompasses the right to exercise free will without external coercion or manipulation by neurotechnology [4 72]. This protects individuals from having their decision-making processes nudge, suppressed, or rewritten by invasive interventions, ensuring ultimate control over their own minds [72]. This principle is directly reflected in prohibitions within regulations like the EU AI Act against AI systems that deploy subliminal techniques to distort behavior [61 62].

The third core principle is the Right to Personal Identity and Psychological Continuity, which safeguards an individual's sense of self, personality, memories, and life narrative from being altered or erased by neurotechnological interventions without profound and informed consent [4 72]. This becomes particularly salient with the rise of closed-loop neurostimulation systems, where long-term modulation of brain activity could potentially reshape a person's identity, a concern raised in studies on the subjective experiences of patients with intelligent BCIs [36 37]. The fourth pillar is the Protection from Algorithmic Bias, which mandates that AI algorithms interpreting neural data must not perpetuate or amplify societal biases related to race, gender, age, or socioeconomic status [4 72]. Research has demonstrated that machine learning models trained on non-representative datasets can produce discriminatory outcomes, such as significantly lower diagnostic accuracy for dermatological conditions in patients with darker skin tones [48]. Finally, the fifth principle is Fair Access to Mental Augmentation, which advocates for the equitable distribution of cognitive enhancement technologies to prevent a new form of social stratification known as the "cognitive divide" [4 72]. Without careful governance, only privileged groups may afford enhancements, exacerbating existing inequalities and undermining distributive justice [72]. Together, these five pillars form a robust framework that directly addresses the fears and aspirations articulated by those seeking to protect their freedom of thought and mental autonomy in an increasingly interconnected world.

Principle	Description	Key Threats Addressed
Mental Privacy	The right to keep one's thoughts, neural patterns, and mental states private from unauthorized collection, surveillance, or use.	Unauthorized decoding of neural signals, covert monitoring, commercialization of brain data, and hacking of BCI devices. [6 72 78]
Cognitive Liberty / Agency	The right to exercise free will and make autonomous decisions without external manipulation or coercion by neurotechnology.	Subliminal influence, behavioral nudging, forced compliance, and suppression of impulses or desires. [4 62 72]
Personal Identity & Psychological Continuity	Protection of an individual's sense of self, personality, memories, and life narrative from alteration by neurotechnological interventions.	Unintended personality changes from neurostimulation, memory modification, and loss of selfhood due to device dependence. [4 36 72]
Protection from Algorithmic Bias	Ensuring that AI algorithms interpreting neural data do not discriminate or impose societal prejudices based on protected characteristics.	Biased diagnoses, inequitable treatment allocation, and exclusionary outcomes for underrepresented populations. [4 48 72]
	Guaranteeing equitable access to technologies that enhance sensory or	Creation of a "cognitive elite," widening of socioeconomic divides,

Principle	Description	Key Threats Addressed
Fair Access to Mental Augmentation	cognitive capacities to prevent social inequality.	and unfair advantages in education and employment. [4 6 72]

Global Legal and Policy Landscapes: From Constitutional Mandates to International Standards

The transition of Neural Rights from a philosophical concept to a binding legal reality has been remarkably swift, driven by pioneering nations and proactive international bodies. This global movement reflects a growing consensus that the unique sensitivity of neural data demands specialized legal protections beyond existing frameworks. The most significant milestone in this evolution was Chile's enactment of a constitutional amendment in October 2021, making it the first country in the world to enshrine Neuro-Rights in its constitution [3 7 82]. Law No. 21.383 amended Article 19 of the Political Constitution to mandate that scientific and technological developments involving cerebral activity and associated data must respect life and physical and psychological integrity [8 80]. This provision effectively establishes "neurodata exceptionalism," recognizing that brain data requires special safeguards even outside of medical contexts [78]. The amendment was championed by Senator Guido Girardi Lavín and developed with input from international scholars, including Dr. Rafael Yuste of the Neurorights Foundation, demonstrating a collaborative effort to translate academic principles into concrete law [8 80]. Following this precedent, Chile’s judiciary provided the first-ever enforcement of these rights in August 2023, when its Supreme Court ruled in a case against the U.S.-based company Emotiv Inc. [78 81]. The court ordered Emotiv to delete brain data collected from a former senator via its Insight headset, finding that the company had violated constitutional rights to physical and psychological integrity and privacy by retaining anonymized data for research without prior, specific consent [8 78]. This landmark judgment serves as a powerful precedent, affirming the need for explicit, revocable consent and rejecting the adequacy of broad adhesion contracts for neurotechnology users [78].

Inspired by Chile's leadership, other nations across Latin America and beyond are actively pursuing similar legal protections. In April 2024, Colorado became the first U.S. state to pass legislation classifying neural data as sensitive personal data under its Consumer Privacy Act, requiring heightened opt-in consent for its collection and processing [4 74 75]. California followed suit later that year, amending its consumer privacy law (CCPA/CPRA) to grant neural data the same protections, taking effect in January 2025 [4 75 77]. These U.S. state-level actions are critical steps toward closing a significant regulatory gap, as federal laws like HIPAA do not cover consumer neurodevices, leaving a vast amount of neural data unprotected [81 93]. Other countries are also advancing legislative initiatives. Brazil has multiple active proposals in Congress, including one to amend its Constitution to include protections for mental integrity and another to classify neurodata as a distinct category of sensitive data under its General Personal Data Protection Law (LGPD) [5 8]. Colombia, Mexico, Argentina, and Uruguay are all considering constitutional or legislative bills to recognize neurorights, signaling a regional trend toward prioritizing cognitive sovereignty [8,73]. In Europe, Spain has incorporated the five proposed neurorights into its Digital Rights Charter, and France has translated OECD recommendations into a national charter for responsible neurotechnology development [6,64].

This wave of national action is supported and guided by international organizations that are working to establish global norms and standards. The Organisation for Economic Co-operation and Development (OECD) issued the first international standard for responsible innovation in neurotechnology in 2019, setting a precedent for ethical governance [8,101]. UNESCO has also been highly active, publishing a report on the ethical issues of neurotechnology in 2022 and a preliminary study in 2023 on a potential standard-setting instrument [4,37]. The Organization of American States (OAS) released the 'Inter-American Declaration of Principles on Neurosciences, Neurotechnologies and Human Rights' in 2023, aligning national frameworks with international standards [4,8]. Furthermore, the UN Human Rights Council tasked its Advisory Committee in 2022 to study the implications of neurotechnology for human rights, underscoring the issue's prominence on the global stage [81]. This concerted international effort is creating a converging set of principles focused on transparency, consent, safety, and fairness, providing a crucial foundation for future global treaties and conventions on Neural Rights. While debates continue among legal scholars about whether new rights are truly necessary versus reinterpreting existing ones, the overwhelming momentum toward codification demonstrates a clear recognition that the brain and mind require a new level of legal protection [81,101].

The Technological Battlefield: Vulnerabilities and Advanced Defense Mechanisms for Neural Data Security

The pursuit of Neural Rights necessitates a deep understanding of the technological landscape, where the very tools meant to enhance human capability also introduce profound security vulnerabilities. Neurotechnologies, particularly Brain-Computer Interfaces (BCIs), operate in a complex environment vulnerable to a wide array of cyberattacks that threaten mental privacy, cognitive liberty, and personal identity. These vulnerabilities span multiple layers of the BCI system, from signal acquisition to cloud storage [57]. At the signal acquisition layer, neural signals are exceptionally weak, typically ranging from $10 - 100$ microvolts (μV), making them highly susceptible to injection of synthetic currents or electromagnetic spoofing, which can disrupt the signal-to-noise ratio and lead to misclassification of intent [57]. An attacker could cause an involuntary prosthetic movement or an unintended action in a virtual environment simply by corrupting the raw neural data stream [57]. The firmware and embedded systems of BCI devices represent another high-risk zone; vulnerabilities in debug ports or insecure bootloader updates could allow an attacker to tamper with the device's code, potentially altering stimulation parameters to deliver harmful electrical currents that could cause neuronal death or hemorrhage [57]. During network communication, data transmitted wirelessly via Bluetooth or Wi-Fi is susceptible to man-in-the-middle (MITM) attacks, where an adversary intercepts and potentially exfiltrates sensitive neural data [12,57]. Even if encrypted, replay attacks—where control packets are re-injected—can disrupt the functionality of closed-loop systems, with a delay of just one second in DBS packets shown to disrupt therapeutic rhythms by up to 23% [57].

The AI and machine learning models that process neural data are also prime targets. Adversarial perturbations, which involve adding minimal noise (<0.2 μV in some bands), can cause false classifications, posing a direct threat to cognitive agency [57]. More insidiously, model poisoning attacks can corrupt training data to degrade system performance or inject backdoors, while model inversion attacks can reconstruct private cognitive states from a model's outputs, directly violating mental privacy [27 57]. Even passive side-channel analysis presents a significant risk; by monitoring electromagnetic emissions, power consumption, or acoustic leakage from a BCI device, an attacker can infer mental states like motor imagery or stress levels without ever accessing the raw neural signal, enabling non-consensual cognitive profiling [57]. These technical threats are not merely theoretical; empirical studies have demonstrated that EEG authentication can be spoofed, and that adversarial perturbations can drop BCI accuracy by 35% [57]. Given these extensive vulnerabilities, the development of advanced defense mechanisms is paramount. The user's request for "unspoofable" protection points directly to a multi-layered security architecture that integrates both software and hardware-based countermeasures.

The defensive arsenal for securing neural data is rapidly evolving, drawing on techniques from cryptography, distributed computing, and computer architecture. A foundational defense is end-to-end encryption (E2EE), which ensures that neural data remains encrypted from the moment it is acquired until it is stored or processed [12 25]. Using strong algorithms like AES-256 and RSA, E2EE prevents unauthorized interception and decryption of data during transmission and storage [25]. Building on this, privacy-preserving computation offers more sophisticated methods for handling data securely. Homomorphic Encryption (HE) allows computations to be performed directly on encrypted data without ever decrypting it, preserving privacy during model training and inference [11]. Secure Multi-Party Computation (SMPC) enables multiple parties to jointly compute a function over their inputs while keeping those inputs private, preventing centralized data breaches [26]. To combat the risks of large-scale data collection, federated learning has emerged as a critical technique. This approach keeps raw EEG data localized on the user's device and only transmits aggregated model updates (gradients) to a central server, thereby minimizing data exposure and reducing the risk of massive data leaks [27 29]. For even greater privacy, differential privacy can be applied, which involves adding calibrated statistical noise to data or model outputs. This provides a formal mathematical guarantee that the presence or absence of any single individual's data in a dataset cannot be determined, effectively preventing re-identification attacks [27 29].

Beyond algorithmic defenses, architectural innovations are crucial for mitigating risks at the hardware level. On-device processing moves complex signal processing tasks, such as spike sorting or feature extraction, directly onto the implantable chip, drastically reducing the volume of data that needs to be transmitted wirelessly [83]. Research has shown that ASIC implementations can achieve a 1866x reduction in data rate compared to conventional systems, dramatically lowering the attack surface [83]. Another innovative approach combines cryptographic protocols with physical layer security. One study proposed a system using metasurface space-time coding to generate harmonic-encrypted beams, camouflaging the information transmission within benign visual stimuli from an EEG headset [10]. This makes it extremely difficult for an adversary to detect or intercept the communication channel, achieving a bit error rate of approximately 50% for eavesdroppers [10]. Collectively, these technologies—from HE and federated learning to on-chip processing and physical-layer encryption—represent the practical realization of the "firewalls" and "protections" needed to enforce Neural Rights. They provide a blueprint for building neurotechnologies that are not only functional but also inherently secure by design.

Layer of BCI System	Primary Vulnerabilities	Advanced Defensive Technologies
Signal Acquisition	Signal Injection, Electromagnetic Spoofing, Sensor Drift Manipulation, Data Interception.	Adaptive Kalman filtering, AES-256 encryption at the source, tamper-resistant hardware design. [12 57]
Firmware & Embedded Systems	Firmware Tampering, Privilege Escalation, Bootloader Injection, Side-channel Leakage.	Secure boot (ECDSA), firmware attestation (TPM 2.0), shielded circuits, randomized task scheduling. [57]
Network Communication	Man-in-the-Middle (MITM) Attacks, Replay Attacks, Data Exfiltration, Protocol Downgrade.	TLS 1.3+ with Perfect Forward Secrecy, X.509 device identity, blockchain audit trails. [12 57]
AI/ML Model Processing	Adversarial Perturbation, Data Poisoning, Model Inversion, Trojan Model Injection.	Adversarial training, differentially private SGD, federated learning, federated security analytics. [27 57]
Side-Channel Analysis	Power Analysis, Timing Analysis, EM Eavesdropping, Acoustic Leakage.	Randomized task scheduling, emission masking, shielded circuits, adaptive Kalman filtering. [57]
Human Interaction	Cognitive Manipulation, Phishing Interfaces, Overload Attacks, Deceptive Alerts.	User awareness training, real-time Bayesian safety alerts, biometric validation, cognitive feedback. [57]

Regulatory Frameworks and Governance Models: Navigating the Patchwork of Existing Laws

The global regulatory environment for neurotechnology is a complex and fragmented patchwork of laws, creating significant challenges for ensuring the protection of Neural Rights. A major point of divergence lies in the distinction between medical-grade devices and consumer-facing neurotechnologies [66 81]. Medical neurotechnologies, such as Deep Brain Stimulation (DBS) systems for Parkinson's disease or implantable BCIs for paralysis, are subject to rigorous oversight by agencies like the European Medicines Agency (EMA) under the EU Medical Device Regulation (MDR) or the U.S. Food and Drug Administration (FDA) [66 93]. These regulations demand extensive pre-market clinical trials, stringent risk management, and adherence to harmonized technical standards, reflecting a focus on patient safety and efficacy [67 70]. However, this high bar of scrutiny does not extend to the burgeoning consumer market for non-medical neurodevices like EEG headsets for meditation, gaming, or productivity tracking [64 81]. These devices often fall under weaker product safety rules rather than medical device regulations, allowing companies to collect highly sensitive neural data with minimal oversight or mandatory impact assessments [66 67]. This regulatory gap creates a high-risk environment where companies can operate with broad discretion over user data, a concern highlighted by the fact that a 2024 report found nearly all online neurotech companies impose no meaningful limitations on their access to or sharing of users' brain data [74].

Existing data protection laws, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), offer a partial solution but face their own limitations. Under GDPR, biometric data used for identification is classified as a "special category," which would likely cover neural data derived from EEG or fMRI scans [46 80]. This affords individuals rights to access, erase, and object to the processing of their data [80]. However, critics argue that GDPR's generalist nature may be insufficient for the unique challenges of neurodata, which can reveal not just identity but also health status, cognitive traits, and political leanings [78]. Similarly, while Colorado and California have amended their consumer privacy acts to explicitly classify neural data as sensitive personal information, their definitions can be ambiguous [75 76]. For example, the Colorado law's definition requires data to be "processed by or with the assistance of a device," potentially excluding inferences drawn from non-device-generated inputs like text sentiment analysis interpreted as neural data [75 76]. Furthermore, exemptions for employee data mean employers could monitor workers' attention or fatigue without full consumer privacy protections, highlighting the need for clearer and more comprehensive legislation [76 77].

In response to these gaps, policymakers and international bodies are developing more targeted frameworks. The EU AI Act, adopted in June 2024, represents a significant step forward by incorporating prohibitions specifically relevant to neurotechnology [62]. It bans the use of AI systems that deploy subliminal or manipulative techniques to distort human behavior, exploit vulnerabilities (especially those related to age or disability), or conduct emotion recognition in workplaces and educational institutions unless for medical purposes [62 65]. It also prohibits biometric categorization systems that infer sensitive attributes like race or political opinions from neural data [61]. While the Act applies piecemeal provisions rather than creating a standalone neurotech regulation, its high-risk classification for many medical AI systems imposes strict requirements on data quality, cybersecurity, and human oversight, which are directly applicable to healthcare neurotechnologies [62 70]. Non-binding policy frameworks, such as the European Charter for the Responsible Development of Neurotechnologies, provide guiding principles for industry, advocating for user-controlled data, transparency, and prohibitions against cognitive manipulation [64 66]. However, their lack of legal force creates enforcement ambiguities, underscoring the need for legally binding regulations. The ongoing debate among legal scholars—whether new, neuro-specific rights are necessary or if existing frameworks can be adapted—is a critical part of this process [81]. Proponents of "neuroexceptionalism" argue that the unique nature of brain data warrants special protections, while opponents warn against "rights inflation" and advocate for strengthening the application of current laws [78 81]. Ultimately, a hybrid approach appears most viable: strengthening existing data protection laws to explicitly cover neurodata and closing loopholes for consumer devices, while continuing to build upon the high-standard framework of medical device regulation to ensure safety and efficacy.

Policy Recommendations and Stakeholder Engagement Strategies for a Rights-Based Future

To effectively protect Neural Rights and translate the principles of cognitive liberty into a functioning legal and ethical ecosystem, a coordinated strategy involving clear policy recommendations and deliberate stakeholder engagement is essential. Policymakers, technologists, and civil society must collaborate to create a governance framework that is both protective and conducive to innovation. A foundational policy recommendation is the universal adoption of granular, dynamic, and informed consent as the cornerstone of all neurotechnology applications. Current consent models, often buried in lengthy "take-it-or-leave-it" adhesion contracts, are inadequate and fail to meet the requirement of being freely given, specific, and informed [76 78]. True consent for neurotechnology requires transparent disclosure of all potential uses, risks, and secondary effects, and must be granular enough to allow users to selectively permit or deny specific types of data processing—for instance, allowing seizure detection while blocking mood analysis [46]. Dynamic controls should enable users to revoke consent in real-time during a BCI session, and post-processing should be strictly limited to the purpose for which consent was originally granted, with repurposing requiring fresh, explicit consent [46 78]. Implementing zero-party consent models, where users proactively share data through preference centers, and adopting interoperable consent portability using standards like W3C Verifiable Credentials can empower users and reduce consent fatigue [46].

Another critical area for policy intervention is the mitigation of algorithmic bias. Regulations must mandate that developers of AI systems used for neurotechnology adhere to rigorous fairness standards throughout the model lifecycle. This includes conducting comprehensive bias audits before deployment and implementing continuous post-deployment monitoring across diverse sociodemographic subgroups [49]. Best practices include ensuring training datasets are representative of intended user populations, using intersectional variables to assess performance, and employing bias mitigation techniques such as data reweighting, adversarial debiasing, and ensemble methods [49 58]. The EU AI Act's requirement for bias audits for high-risk AI systems provides a strong model for such obligations [46]. Furthermore, policies should promote the development and adoption of Explainable AI (XAI) techniques to increase transparency and accountability. XAI methods like SHAP and LIME can help explain why a model made a particular prediction, fostering trust and allowing for the identification of biased decision-making [45 47]. Counterfactual explanations, which show what changes would have led to a different outcome, are particularly valuable for demonstrating procedural fairness in adverse decisions, aligning with legal requirements for meaningful information [44].

Effective implementation of these policies requires robust stakeholder engagement. Affected individuals and advocacy groups must be included in regulatory consultations to ensure that policies reflect lived experiences and address genuine concerns [13]. Public education campaigns are vital to raise awareness about Neural Rights and empower users to protect their own data [46]. For technologists and industry, partnerships with advocacy groups can foster compliance and encourage the integration of ethical design principles, or "neurodata by design," into product development cycles from the outset [46,64]. Providing open-source consent management frameworks and promoting up-to-date training on data handling can lower barriers to compliance [46]. Policymakers and regulators should facilitate multi-stakeholder dialogues, support the development of international standards, and resourcing independent oversight bodies to enforce these new rights [46]. To summarize, the path forward involves a three-pronged approach: legislating for robust, user-centric consent and bias mitigation; mandating transparency through XAI and public reporting; and building a coalition of engaged stakeholders to drive both policy development and corporate responsibility. By championing these principles, society can begin to build an ethical foundation that respects human cognitive autonomy in an era of accelerating neurotechnology, transforming the struggle for freedom of thought into a universally recognized and defended human right.

Reference

1. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA
2. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA
3. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA
4. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

5. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

6. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

7. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

8. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

9. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlbl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVybFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

10. Secure wireless communication of brain – computer ... https://www.nature.com/articles/s41467-025-63326-0

11. End-to-End Encrypted Neural Networks for Secure ... https://medium.com/aardvark-infinity/end-to-end-encrypted-neural-networks-for-secure-communication-a-revolutionary-approach-to-secure-b795b86ee901

12. Cybersecurity for Brain-Computer Interfaces https://akitra.com/cybersecurity-for-brain-computer-interfaces/

13. BCI Technical and Policy Recommendations to Mitigate ... https://fpf.org/blog/bci-technical-and-policy-recommendations-to-mitigate-privacy-risks/

14. Notices of Funding Opportunities - BRAIN Initiative - NIH http://braininitiative.nih.gov/funding/funding-opportunities
15. Funding for Brain-Computer Interface Ventures https://www.from-the-interface.com/bci-venture-funding/
16. N3: Next-Generation Nonsurgical Neurotechnology https://www.darpa.mil/research/programs/next-generation-nonsurgical-neurotechnology
17. Understanding the Brain https://www.nsf.gov/focus-areas/brain
18. Funded Awards | BRAIN Initiative - NIH http://braininitiative.nih.gov/funding/funded-awards
19. Brain − Machine Interface Projects https://brain.ieee.org/brain-topics/brain-machine-interface-projects/
20. USC researchers receive funding to develop next generation ... https://keck.usc.edu/news/usc-researchers-receive-funding-to-develop-next-generation-of-intelligent-biocomputers/
21. Democratizing open neuroimaging: Neurodesk's approach ... https://apertureneuro.org/article/144107-democratizing-open-neuroimaging-neurodesk-s-approach-to-open-data-accessibility-and-utilization
22. Can Open-source Neurotech Hardware Make It Accessible ... https://www.youtube.com/watch?v=QnKVQwRzT1g
23. brainlife.io: a decentralized and open-source cloud ... https://www.nature.com/articles/s41592-024-02237-2
24. Neuroscience Cloud Analysis As a Service: An open- ... https://www.sciencedirect.com/science/article/pii/S0896627322005876
25. Privacy and security concerns | Brain-Computer Interfaces ... https://fiveable.me/brain-computer-interfaces/unit-12/privacy-security-concerns/study-guide/FoDbqmvfNf46GRAW
26. Protecting Privacy of Users in Brain-Computer Interface ... https://www.researchgate.net/publication/334286648_Protecting_Privacy_of_Users_in_Brain-Computer_Interface_Applications
27. Securing Brain-Computer Interfaces: Machine Learning ... - ijrpr https://ijrpr.com/uploads/V6ISSUE10/IJRPR54208.pdf
28. Privacy Preserving Classification of EEG Data Using ... https://www.mdpi.com/2076-3417/11/16/7360
29. DSpace JSPUI - Lakehead Knowledge Commons https://knowledgecommons.lakeheadu.ca/jspui/handle/2453/5394
30. Interoperability standards in digital health https://www.medtecheurope.org/wp-content/uploads/2021/10/mte_interoperability_digital_health_white-paper_06oct21.pdf
31. A Scoping Review of Emerging Technologies and ... https://www.mdpi.com/1660-4601/22/10/1535

32. Designing Guiding Systems for Brain-Computer Interfaces https://pmc.ncbi.nlm.nih.gov/articles/PMC5535189/
33. Guiding principles and considerations for designing a well- ... https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2025.1554266/full
34. Brain – computer interfaces: the innovative key to unlocking ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11392146/
35. Advancing Brain-Computer Interface Closed-Loop Systems for ... https://biomedeng.jmir.org/2025/1/e72218
36. Application and future directions of brain-computer ... https://www.sciencedirect.com/science/article/pii/S2589238X2500083X
37. The functional differentiation of brain – computer interfaces ... https://www.nature.com/articles/s41599-023-02419-x
38. Personalized Brain – Computer Interface and Its Applications https://www.mdpi.com/2075-4426/13/1/46
39. Using brain-computer interfaces: a scoping review of studies ... https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-019-0354-1
40. Five Levels of Explanation (Part II): How Brain-Computer ... https://arctop.com/deep-dives/how-bci-works-part-2
41. Cognitive Load and Explainability in Human-Centered ... https://medium.com/design-bootcamp/cognitive-load-and-explainability-in-human-centered-explainable-artificial-intelligence-b108d03b293c
42. The application of eXplainable artificial intelligence in ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11427810/
43. Exploring the Impact of Explainable AI and Cognitive ... https://arxiv.org/html/2505.01192v1
44. Explainable AI as evidence of fair decisions https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1069426/full
45. Explainable AI: Bridging the Gap Between Human ... https://pg-p.ctme.caltech.edu/blog/ai-ml/explainable-ai-bridging-gap-between-human-cognition-and-ai-models
46. Neurodata Consent Frameworks: Managing EEG/Brain ... https://secureprivacy.ai/blog/neurodata-consent-eeg-brain-computer-interface-data-gdpr-ccpa
47. ARTIFICIAL INTELLIGENCE IN MODERN FIREWALLS https://trepo.tuni.fi/bitstream/handle/10024/161576/AhmadWajeh.pdf?sequence=2
48. The Sociodemographic Biases in Machine Learning ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11204917/
49. Sociodemographic bias in clinical machine learning models https://www.sciencedirect.com/science/article/pii/S0895435624003627

50. Study of an Optimization Tool Avoided Bias for Brain ... https://www.sciencedirect.com/science/article/pii/S1959031824000174
51. Biases in BCI experiments: Do we really need to balance ... https://www.frontiersin.org/journals/computational-neuroscience/articles/10.3389/fncom.2022.900571/full
52. Towards identifying optimal biased feedback for various ... https://arxiv.org/pdf/2112.12399
53. Biased feedback in brain-computer interfaces https://jneuroengrehab.biomedcentral.com/articles/10.1186/1743-0003-7-34
54. (PDF) Biased feedback in brain-computer interfaces https://www.researchgate.net/publication/45364977_Biased_feedback_in_brain-computer_interfaces
55. A multi-day and high-quality EEG dataset for motor imagery ... https://www.nature.com/articles/s41597-025-04826-y
56. bigP3BCI: An Open, Diverse and Machine Learning Ready ... https://physionet.org/content/bigp3bci/
57. Powered Brain − Computer Interfaces https://verjournal.com/index.php/ver/article/download/522/425/1108
58. Bias Detection and Mitigation Framework https://www.emergentmind.com/topics/bias-detection-and-mitigation-framework
59. Cybersecurity in Brain-Computer Interfaces: RFID-based ... https://www.researchgate.net/publication/348016726_Cybersecurity_in_Brain-Computer_Interfaces_RFID-based_design-theoretical_framework
60. Confronting Bias: BSA's Framework to Build Trust in AI https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai
61. Neurotechnologies under the EU AI Act: Where law meets ... https://iapp.org/news/a/neurotechnologies-under-the-eu-ai-act-where-law-meets-science
62. Implications of the novel EU AI Act for neurotechnologies https://www.sciencedirect.com/science/article/pii/S089662732400607X
63. Article 11: Technical Documentation https://artificialintelligenceact.eu/article/11/
64. European-Charter-for-the-Responsible-Development-of- ... https://www.braincouncil.eu/wp-content/uploads/2025/04/European-Charter-for-the-Responsible-Development-of-NeuroTechnologies-FINAL.pdf
65. High-level summary of the AI Act https://artificialintelligenceact.eu/high-level-summary/
66. EU Policy & Regulatory | Neurotech https://www.considerati.com/publications/neurotechnology-in-the-eu-balancing-innovation-with-rights-based-regulation/
67. The new regulation of non-medical neurotechnologies in the ... https://pmc.ncbi.nlm.nih.gov/articles/PMC11424214/

68. TechDispatch #1/2024 - Neurodata https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata
69. AI Act: what are the implications for sensitive sectors in ... https://www.polytechnique-insights.com/en/columns/digital/ia-act-what-are-the-implications-for-sensitive-sectors-in-europe/
70. Setting the Standard: The EU AI Act's Impact on Healthcare AI https://roninlegalconsulting.com/policy-brief-harmonised-standards-for-the-eu-ai-act/
71. Neuro-adaptive architecture: Buildings and city design that ... https://www.sciencedirect.com/science/article/pii/S2590051X24000315
72. Neuro-Rights → Term https://lifestyle.sustainability-directory.com/term/neuro-rights/
73. Literature Review: Neurotechnology https://www.nuffieldbioethics.org/wp-content/uploads/Neurotechnology-Literature-Review-WEB-FINAL.pdf
74. States Pass Privacy Laws To Protect Brain Data Collected ... https://kffhealthnews.org/news/article/colorado-california-montana-states-neural-data-privacy-laws-neurorights/
75. California and Colorado Establish Protections for Neural ... https://www.afslaw.com/perspectives/alerts/california-and-colorado-establish-protections-neural-data
76. “Key Issues Raised by Colorado's Brain Data Privacy Bill ... https://www.alston.com/en/insights/publications/2024/04/key-issues-raised-by-colorado
77. Colorado and California Get Ahead of Neural Data ... https://www.bakerdatacounsel.com/blogs/colorado-and-california-get-ahead-of-neural-data-regulation/
78. Chilean Supreme Court ruling on the protection of brain ... https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2024.1330439/full
79. Chile: Pioneering the protection of neurorights https://courier.unesco.org/en/articles/chile-pioneering-protection-neurorights
80. Mind the Gap: Lessons Learned from Neurorights https://www.sciencediplomacy.org/article/2022/mind-gap-lessons-learned-neurorights
81. The Controversial Push for New Brain and Neurorights https://www.jmir.org/2025/1/e72270/
82. Neurotechnology and the Law: A Legal Perspective - Clio https://www.clio.com/blog/neurotechnology-law/
83. Frameworks for Efficient Brain-Computer Interfacing https://amir.sdsu.edu/Valencia19Frameworks.pdf
84. System Architecture for Brain-Computer Interface based on ... https://thesai.org/Downloads/Volume13No3/Paper_57-System_Architecture_for_Brain_Computer_Interface.pdf
85. View Grant Opportunity https://grants.gov/search-results-detail/352467
86. View Grant Opportunity https://www.grants.gov/search-results-detail/302121

87. Six Paths to the Nonsurgical Future of Brain-Machine ... https://www.darpa.mil/news/2019/nonsurgical-brain-machine-interfaces
88. Team Receives $19 Million from DARPA To Create ... https://www.cmu.edu/news/stories/archives/2019/may/darpa-brain-interface.html
89. DARPA Announces that Six Teams Will Receive Funding ... https://www.battelle.org/insights/newsroom/news-details/2021/09/09/darpa-announces-that-six-teams-will-receive-funding-under-the-next-generation-nonsurgical-neurotechnology-(n3)-program
90. DARPA Funds Brain-Machine Interface Program https://singularity2030.ch/darpa-funds-brain-machine-interface-program/
91. BRAIN Initiative: Next-Generation Devices for Recording ... https://grantexec.com/grants/da71446d-472b-4341-9548-94019e388744
92. How DARPA drives Brain Machine Interface Research https://www.from-the-interface.com/darpa-funding-bci-research/
93. Annex 9.6 National Legal Case Study: Neurotechnologies ... https://www.techethos.eu/wp-content/uploads/2023/02/TechEthos-D4.2-National-Legal-Case-Study_Neurotechnologies_USA_watermarked.pdf
94. An integrated brain-machine interface platform with ... https://www.researchgate.net/publication/335505633_An_integrated_brain-machine_interface_platform_with_thousands_of_channels
95. Advancements and challenges in brain-computer interfaces https://www.the-innovation.org/article/doi/10.59717/j.xinn-life.2024.100058
96. Integrating simultaneous motor imagery and spatial attention ... https://pmc.ncbi.nlm.nih.gov/articles/PMC10803074/
97. An Integrated Brain-Machine Interface Platform With ... https://www.jmir.org/2019/10/e16194/citations
98. Cybersecurity in Brain-Computer Interfaces: RFID-based ... https://www.sciencedirect.com/science/article/pii/S2352914820306407
99. Computer Architecture for Brain-Computer Interfaces https://www.sigarch.org/computer-architecture-for-brain-computer-interfaces/
100. Integrating the Brain − Computer Interface and Building ... https://www.diva-portal.org/smash/get/diva2:1917794/FULLTEXT01.pdf
101. On Neurorights - PMC https://pmc.ncbi.nlm.nih.gov/articles/PMC8498568/
102. Mental Privacy in the Age of Neurotechnology Author https://repository.gchumanrights.org/server/api/core/bitstreams/7c74891d-a5bb-4dd4-94bf-06337fd6f021/content