

Protecting Human Rights in the Age of Neurotechnology: Mental Privacy and Mental Security

Hadiza Musa

Policy Brief
December 2024

While existing human rights frameworks, such as the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) (e.g., Article 17: Right to privacy), address privacy and security concerns, they do not explicitly cover mental privacy and security issues posed by neurotechnology. This governance gap is critical given the rapid growth of neurotechnologies, from medical benefits to risks in commercial applications like brain-computer interfaces (BCIs). Mental privacy and security, fundamental to our humanity and autonomy, require safeguards to protect individual rights while fostering innovation and equity. We propose introducing new rights for mental privacy and security through a collaborative approach involving governments, businesses, and communities.

Supporting References

Mental privacy and mental security, while closely related, address distinct risks to the brain. Mental privacy rights refer to individuals' control over access to their neural data and the information derived from it,¹ while neurosecurity involves protecting neural devices from malicious interference to safeguard neural integrity, computation, and free will.² Current human rights frameworks lack the specificity to address these unique risks. Scholars³ and neuro-rights advocates⁴ highlight critical governance gaps in the existing frameworks.

- Lack of individual protection from private businesses and government players' unauthorized collection and commodification of neural data.
- Failure to regulate the use of neuro-surveillance tools that can extract or affect thoughts, emotions, or intentions without consent.

¹ Wajnerman Paz A. "Is Mental Privacy a Component of Personal Identity?" *Front Hum Neurosci.* (2021): 15:773441. doi: 10.3389/fnhum.2021.773441

² Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. "Neurosecurity: security and privacy for neural devices", *Neurosurgical Focus FOC* 27, 1 (2009): E7, doi: <https://doi.org/10.3171/2009.4.FOCUS0985>

³ Ienca, Marcello, and Roberto Andorno. "Towards new human rights in the age of neuroscience and neurotechnology." *Life sciences, society and policy* vol. 13,1 (2017): 5. doi:10.1186/s40504-017-0050-1

⁴ Yuste, R. and Goering, S. (2017) 'Four ethical priorities for neurotechnologies and AI', *Nature*, 551(7679), p. 159. Available at: <https://doi.org/10.1038/551159a>.

- Lack of accountability for potential abuse of neurotechnology in contexts such as the judiciary, employment, law enforcement, or advertising sectors.

The implications of these governance gaps pose the following mental privacy and security risks:

- **Data Misuse:** One of the most significant mental privacy risks is that neural data, far more sensitive than biometric or personal data, could be extracted and exploited for commercial use, government neuro-surveillance, profiling, or manipulation without individuals' awareness or consent.
- **Hacking of Neural Devices:** The risk that arises from mental security is that vulnerability in neural implants, and interfaces could allow ill-intent actors to control or disrupt cognitive processes, posing risks to personal security and autonomy.
- **Discrimination:** Neural data could reinforce biases, leading to exclusion based on inferred traits, beliefs, or emotional states, which could threaten mental privacy and security.

These risks highlight the urgent need for targeted provisions to protect mental privacy and security, which are integral to existing human rights frameworks.

Real-World Examples

The rapid development of BCIs highlights challenges in mental privacy. While BCIs assist individuals with disabilities by recording neural signals to facilitate communication or control devices, they also collect sensitive neurodata, raising concerns about misuse. In workplaces, wearable neurotech monitoring fatigue or focus could be exploited for hiring or promotion decisions, violating privacy. Similarly, consumer devices like the Muse headband, which uses EEG sensors to monitor brain activity, fall outside medical regulations, allowing companies to collect and sell brain data without oversight.⁵ These examples underscore the urgent need for governance mechanisms to secure neurodata and address gaps in human rights protections.

Expected Outcomes

The neurotechnology market is projected to grow to \$50.2 billion by 2032, with a sizeable share of devices designed for consumer use.⁶ Without global standards, the risks to privacy and security will rise exponentially. To address these challenges, we propose the introduction of two rights that extend and modernize existing privacy and security principles:

- **The Right to Mental Privacy**

The Right to Mental Privacy guarantees individuals full control over their neural data and prohibits the non-consensual collection, storage, analysis, or sharing of such data by any entity. It also restricts the use of neuro-surveillance technologies to infer cognitive states without explicit,

⁵ Samuel, Sigal. 2024. "Your Brain's Privacy Is at Risk. The US Just Took Its First Big Step Toward Protecting It." Vox, April 18, 2024. <https://www.vox.com/future-perfect/24078512/brain-tech-privacy-rights-neurorights-colorado-yuste>.

⁶ Ltd, Sns Insider Pvt. 2024. "Neuroscience Market Projected to Reach USD 50.2 Billion by 2032, Growing at a 4.0% CAGR – S&S Insider." GlobeNewswire News Room, November 11, 2024. <https://www.globenewswire.com/news-release/2024/11/11/2978478/0/en/Neuroscience-Market-Projected-to-Reach-USD-50-2-Billion-by-2032-Growing-at-a-4-0-CAGR-S-S-Insider.html>.

informed consent. Neural data should be legally recognized as a distinct category of highly sensitive personal data under international law. Given its unprecedented intimacy: revealing thoughts, intentions, and emotional states, its misuse poses direct risks to autonomy, dignity, and democratic participation.

Accordingly, this right requires:

- Explicit and informed consent for all data collection and processing
- Strict limitations on secondary use or commercialization of neural data
- Clear liability mechanisms for unauthorized access, profiling, or exploitation

The right to mental privacy has the potential to modernize existing privacy principles to address the unique vulnerabilities introduced by neurotechnology.

- **The Right to Cognitive Security**

This right safeguards individuals against external interference with their neural systems. It includes protections against unauthorized access to neural implants or interfaces and against manipulating cognitive processes for ill-intent uses, such as altering thoughts, decisions, or emotional states. The goal is to protect individuals against the manipulation or hacking of neural systems. We propose a Mandate of minimum technical security standards for neurotechnology, with independent oversight. If neural security standards are adopted, then neurotechnology innovation can grow responsibly. All neurotechnologies must meet stringent security standards to prevent unauthorized access, hacking, or coercion. Together, these rights bridge the gap between existing privacy protections and the unique threats introduced by neurotechnology. The scope of these rights includes data protection, informed consent, and accountability for misuse. They build on principles already enshrined in Article 12 of the UDHR and Article 17 of the ICCPR while tailoring them to address the new-age technology challenges.

To achieve these rights, we recommend a coordinated effort across sectors:

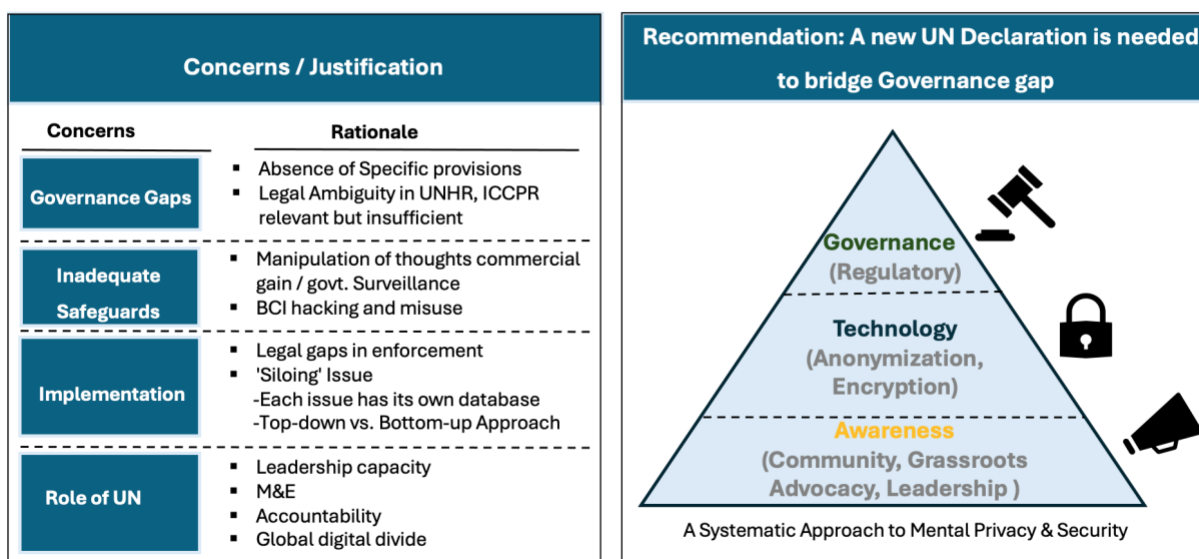
- **Legislative Action:**
 - The UN should continue its UNESCO 2025 plan to define a Global Neurodata Framework that includes data minimization principles and standards for cross-border data sharing.
 - Governments should establish legal frameworks incorporating mental privacy and cognitive security as fundamental rights (such as the Chile case study).
 - These frameworks should define explicit liabilities for violations and set rigorous consent standards for using neurotechnology.
- **Technological Standards:**
 - Technology companies must embed human rights principles into the design and deployment of neurotechnologies. They must also introduce strict consent protocols,

such as tiered consent systems, where individuals have granular control over their neural data access and use.

- Global ethical standards should be developed to ensure transparency, fairness, and accountability, such as using ISO-like certifications for neural device security and ensuring compliance with best practices.
- Establish precise liability mechanisms for misuse.
- **Community Engagement:**
 - Civil society organizations and local communities should play a key role in shaping governance mechanisms and ensuring inclusivity and equity.
 - Educational initiatives should raise public awareness about the implications of neurotechnology and the importance of mental privacy.

To achieve these rights and mitigate risks effectively, a multi-stakeholder approach involving governments, the private sector, and civil society is necessary. A global framework ensures equitable access to secure and ethical neurotechnology, benefiting medicine while protecting individuals from the risks of cognitive enhancement tools. Protecting mental privacy and security is not merely a matter of individual rights but a prerequisite for preserving trust, autonomy, and equality in the global digital space. Including these provisions in a new declaration should lead to a worldwide effort by the United Nations to ensure neurotechnology enhances humanity without compromising its dignity. We call upon UN member states, governments, industry leaders, and civil society to prioritize these recommendations and work collaboratively to build a future where innovation aligns with the core values of human rights.

Mental Privacy and Security- Current Human Rights inadequately address Mental privacy and security risks posed by Neurotech



Best Practices and Policy Developments

- European Union (2018–2024)

The EU's GDPR marked a critical step in digital data privacy. In July 2024, the European Parliament published a study on mental privacy protections, emphasizing the need for legal safeguards in neurotechnology.⁷

- OECD Standards (2019)

The Organization for Economic Cooperation and Development (OECD) developed the first international standards addressing neurotechnology's ethical, legal, and social challenges through its Recommendation on Responsible Innovation in Neurotechnology.⁸

- Chile (2021)

Chile became the first country to amend its Constitution to protect mental integrity and neuro data. The law ensures that brain activity and its derived information are safeguarded and mandates scientific and technological developments that respect physical and mental integrity.⁹

- Latin America (2024)

Neuro-privacy initiatives have spread across Latin America. As of March 2024, Mexico is considering two neuro-privacy bills proposed by Deputy María Eugenia Hernández Pérez to protect psychological integrity and identity. In Brazil, several neuro-privacy measures are gaining traction.¹⁰

- United States (2024)

Colorado enacted the nation's first neurodata protection law in April, followed by California's landmark law in October.¹¹ California's law allows users to control neural data collected by neurotech companies. This includes the right to request, delete, correct, or limit data collection and opt out of data sharing or sales.¹²

- Geneva Academy and UN Efforts

Institutions like the Geneva Academy, the University Neuro-center, and the UN HRC Advisory Committee are working to empower stakeholders with a shared understanding of neurotechnology risks. Their goal is to strengthen international human rights frameworks and foster effective regulation.¹³

⁷ GDPR.eu. 2019. "General Data Protection Regulation (GDPR) Compliance Guidelines." February 19, 2019. <https://gdpr.eu/>.

⁸ "OECD Legal Instruments." n.d. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457>.

⁹ "Chile — the Neurorights Foundation." n.d. The Neurorights Foundation. <https://neurorightsfoundation.org/chile>.

¹⁰ "Privacy and the Rise of 'Neurorights' in Latin America - Future of Privacy Forum." n.d. Future of Privacy Forum. <https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/>

¹¹ "Neural Data Privacy an Emerging Issue as California Signs Protections Into Law." n.d. The Record From Recorded Future News. <https://therecord.media/neural-data-privacy-california-law-yuste>

¹² "Senate Overwhelmingly Approves Nation's Strongest Neurorights Bill." 2024. Senator Josh Becker. May 21, 2024. <https://sd13.senate.ca.gov/news/press-release/may-21-2024/senate-overwhelmingly-approves-nations-strongest-neurorights-bill>.

¹³ "Neurotechnology and Human Rights - the Geneva Academy of International Humanitarian Law and Human Rights." n.d. <https://www.geneva-academy.ch/research/our-clusters/digitalization-and-new-technologies/detail/105-neurotechnology-and-human-rights>.

References

"Chile the Neurorights Foundation." n.d. The Neurorights Foundation.

Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. "Neurosecurity: security and privacy for neural devices", *Neurosurgical Focus FOC* 27, 1 (2009): E7

GDPR.eu. 2019. "General Data Protection Regulation (GDPR) Compliance Guidelines." February 19, 2019

Ienca, Marcello and Roberto Andorno. "Towards New Human Rights in the Age of Neuroscience and Neurotechnology." *Life Sciences, Society and Policy* 13, no. 1 (April 26, 2017): 5. doi:10.1186/s40504-017-0050-1

Ltd, Sns Insider Pvt. 2024. "Neuroscience Market Projected to Reach USD 50.2 Billion by 2032, Growing at a 4.0% CAGR – S&S Insider." *GlobeNewswire News Room*, November 11, 2024.

"Neural Data Privacy an Emerging Issue as California Signs Protections Into Law." n.d. *The Record From Recorded Future News*.

"Neurotechnology and Human Rights - the Geneva Academy of International Humanitarian Law and Human Rights." n.d.

"OECD Legal Instruments." n.d.

"Privacy and the Rise of 'Neurorights' in Latin America - Future of Privacy Forum." n.d. *Future of Privacy Forum*.

Samuel, Sigal. 2024. "Your Brain's Privacy Is at Risk. The U.S. Just Took Its First Big Step Toward Protecting It." *Vox*, April 18, 2024.

"Senate Overwhelmingly Approves Nation's Strongest Neurorights Bill." 2024. *Senator Josh Becker*. May 21, 2024.

Wajnerman Paz A. "Is Mental Privacy a Component of Personal Identity?" *Front Hum Neurosci.* (2021): 15:773441.

Yuste, R. and Goering, S. (2017) 'Four ethical priorities for neurotechnologies and AI', *Nature*, 551(7679), p. 159