

Towards a Neurodata Protection Framework in Australia

Raphaella Revis

School of Law and School of Computer Science
University of Technology Sydney
Ultimo, Australia
raphaella.revis@student.uts.edu.au

Avinash Singh

School of Computer Science
University of Technology Sydney
Ultimo, Australia
avinash.singh@uts.edu.au

Abstract—Neurotechnology enables the recording, interpretation and modulation of neural activity, generating and extracting highly sensitive neural data with significant privacy implications. While jurisdictions worldwide have begun addressing neurodata governance and regulation through constitutional reform, sector-specific legislation and enhanced privacy protections, Australia currently lacks a framework to explicitly safeguard neurodata. This paper examines the current limitations of Australia’s existing privacy regime in addressing neurotechnology related risks, including re-identification, unauthorized secondary use, neuro-marketing and cybersecurity breaches. Drawing on comparative developments in the United States, Chile, and Mexico, the paper proposes the first Neurodata Privacy Protection Framework (NPPF) designed to Australia’s legal context. The NPPF adopts a more soft-law approach but is aligned with the Australian Privacy Principles (APPs) embedded in statute, emphasizing informed consent, mental privacy, pseudonymization and data security. To evaluate the framework’s effectiveness, a simulated case study is applied, demonstrating how the NPPF may mitigate harms identified in Australia. The proposed NPPF is practical and scalable model for neurodata governance without requiring strenuous Australian constitutional reform while also offering significant benefits for current and future neurodata protection.

Index Terms—neurotechnology, neurodata, privacy, brain-computer interface, regulatory framework, neurorights

I. INTRODUCTION

Neurodata has emerged as a highly personal and sensitive form of data, leading to debate on legal categorisation and information security. Functionally enabled by neurotechnologies such as brain-computer interfaces (BCIs), neurodata is increasingly used in contexts beyond initial medical spaces as consumer application such as gaming [1], neuromarketing [2], and cognitive-performance monitoring [3], [4]. These applications raise important concerns about the extent to which individuals can give informed and meaningful consent to the collection and use of their neural data, as highlighted by the United Kingdom Information Commissioner [5]. Implantable BCIs, such as those developed by Synchron and Neuralink’s devices [6], demonstrate a significant potential of neurodata in clinical and rehabilitation applications [7]. These developments offer significant benefits, particularly in healthcare, where they may support the treatment of neurological conditions [8] and the restoration of sensory functions [9]. However, they also generate unprecedented legal and ethical concerns. Unlike other forms for personal information, neurodata has potential

to expose an individual’s cognitive states, intentions, and/or personal information beyond what is specifically requested during an initial purpose [10].

Globally, the landmark Chilean Supreme Court case *Girardi v Emotiv* illustrated the risks of neurodata stemming from insufficient guidelines and security protocols [11] compromising personal data. The case became the tipping point for Chilean reform, prompting international discussion due to the multi-layered issues it revealed [12]. Even when data is seemingly de-identified, neurodata still remains vulnerable to re-identification, commodification [2], cyber breaches [11] and unauthorized secondary uses. These concerns are shared by scholars [11], [13], which also echo in *Girardi v Emotiv* findings.

In light of these risks, the question becomes whether Australia’s existing privacy and regulatory settings are equipped to address these emerging neurodata risks. Australia’s current privacy framework does not explicitly recognize neurodata as a distinct category of sensitive information. Recently, United Nations Educational, Scientific and Cultural Organization (UNESCO) announced the launch of a world-first framework to establish a unified standard in neurotechnology management that puts human rights at the forefront [14]. It is anticipated that UNESCO works with Member States to introduce necessary policies, and Australia is a member since 1946. However, no such comparable framework currently exists in Australia, despite growing research and commercial interest in neurotechnology [15]. A limited market scale, with only about 100 companies, may be one of the reasons for the lack of momentum behind the reforms needed in Australia. At the same time, international activities demonstrates that regulatory change is often triggered by judicial intervention such as seen in *Girardi v Emotiv*, although industry debate had already been active [12]. Consequently, the Australian Human Rights Commission (AHRC) has expressed concern about the lack of explicit guidelines or legislation to particularly safeguard against neurodata misuse [3], in light of increased adoption [2]. This paper therefore proposes the first neurodata protection framework for Australia to establish clear standards for neurodata collection, handling and security, thereby promoting transparency and strengthening user trust.

II. COMPARATIVE DATA PRIVACY LANDSCAPES IN AUSTRALIA AND AMERICAN REGIONS

A. Australian Landscape

Scientific advances have accelerated the proliferation of emerging technologies, such as artificial intelligence (AI) [16], reshaping how data is generated. Among these technologies, neurotechnology is especially data-intensive, relying on data for input, operation and output [17], making privacy law the most suitable and aligned regulatory lens due to its unifying principles across jurisdictions in Australia. The Therapeutic Goods Administration (TGA), an Australian government regulatory body responsible for the certification and regulation of medical devices, has recently published a consultation on the need to strengthen AI-fueled medical devices. The consultation paper is unclear whether neurotechnology falls within the proposed AI-related changes [18]. Nevertheless, regulation of neurotechnology use does not in and of itself protect misuse of the neurodata nor address privacy concerns.

The current Australian legal privacy protection is the *Privacy Act 1988 (Commonwealth)* [19], governing collection, handling, and access of personal information across public and private sectors. It is supplemented by the APPs contained in Schedule 1 [20]. The APPs are a supplementary guide for organizations to ensure personal information is handled in a safe manner that considers technology broadly but non-specifically [21]. The *Privacy Act 1988* was introduced following an Australian Law Reform Commission inquiry to give effect to international obligations such as Article 17 of the International Covenant on Civil and Political Rights [22]. Consequently, the *Privacy Act 1988* adopts a rights-based approach centered on individual autonomy and morality [23]. The *Privacy Act 1988* has evolved through considerable amendments, including the establishment of the Office of the Australia Information Commission in 2010 [24], the introduction of a notifiable data breach scheme [25], and most recently, a statutory tort of serious invasion of privacy [26]. The first case under the new tort [27], tried in October 2025 in the New South Wales District Court, emphasized the deeply personal nature of digital data, signaling that Australia is taking privacy more seriously than ever. However, further steps are needed for rapidly adopted technologies like neurodata as the byproduct of neurotechnology.

B. US landscape

Unlike Australia, US human rights are expansive and cannot be easily amended by ordinary legislators due to the US rule of 'supermajority' amendment [28]. Further, there is no federal privacy law equivalent to the Australian *Privacy Act 1988*, instead focusing on individual legislation and regulations on different areas of privacy in the US. As scholars outlined in an analysis on American consumer laws, the *Colorado Privacy Act* (CPA) is one of the comprehensive individual state laws in addition to California [29] which is particularly important in the context of neurotechnology. In the absence of a comprehensive federal privacy regime, data-related risks

arising from neurotechnology in the US are to be addressed through fragmented privacy and consumer protection laws at state level [30]. Consequently, data governance challenges become at the forefront of regulatory responses, as privacy law is the primary mechanism through which neurodata is indirectly regulated.

C. South/Latin America Landscape

Distinguished from the Australian and US laws, South/Latin American legal systems focus on entrenchment of rights, which is evidenced in Chile's landmark decision in *Girardi v Emotiv* to embed neurorights as an individual's right to neural data in the Constitution. Contrarily, Colorado in the US opted to include similar characteristics in their state-level privacy legislation. In relation to data protection more broadly, Chile recently approved Law 21.719 on Protection of Personal Data (LPPD), effective from December 2026 [31]. This legislation aims to build on and reform the previous legislation considered a data protection framework by being fit-for-purpose for emerging technologies like neurotechnology and global standards. A key provision in this upcoming legislative framework is the establishment of a data protection authority, enhanced data rights and additional bases for data processing particularly around the issues of consent. Under the LPPD, data can be anonymized or pseudonymized, similarly to the European General Data Protection Regime (GDPR) [32]. Both pseudonymization and anonymization are defined differently in the Chilean law – one being a process that does not attribute data to the "data subject/natural person", and the other an "irreversible process" respectively. Under this provision, pseudonymized data would only be personal data if it can be identifiable with additional information. These practices are not always viable for each type of data. As per Eke et al [?] pseudonymization is a costly process and a hindrance to research. The issue of re-identification is also significant as emphasized by the UK ICO [5], requiring the process to be fully completed. Considering that research relies on data, particularly in the neurodata space, such a provision may be controversial [33].

III. GOVERNING NEURODATA

Neurotechnology, and its neurodata, have been dubbed as a technology frontier [34] largely due to the immense therapeutic and consumer benefits that it can present. This characterization is attributed to the technologists' capability of measuring, accessing, analyzing or predicting human nervous system activity [35], and consequent potential to augment and manipulate neurodata [34]. BCIs in particular enable vulnerable individuals who may have certain neurological impairments like locked-in-syndrome able to perform motor activity via brain activity [36]. Despite these practical benefits, misuse of neurodata from the technology can lead to harms such as depletion of mental privacy [37]. At the same time, researchers [38] warn against an overhype of harms, with a need for balance and cautionary principles instead otherwise it may create a negative effect on innovation in the field.

Medical research experts speculate that mind-body integrated therapeutics will be greatly assisted by neurotechnology in the near future [39] with even further advancements by 2035 [40].

Farahany in *The Battle for Your Brain* [13], a leading scholar on the legal aspect of neurotechnology and neurodata, argues that banning neurodata collection is inefficient as it deprives those in need from access to essential assistance. Given that neurodata are inherently invasive brain data, it naturally falls under privacy law as consensual collection or manipulation is an invasion of personal space. In response, many countries have acted to either legislate or regulate neurodata because of the sensitive nature [30]. Arguably, the recently proposed US MIND Act [41] aims to address the area on a country level. The proposed MIND Act seeks to ensure data remains private through extending privacy concepts instead of creating an entirely new regime. As noted above, the US does not currently have uniform federal privacy laws, which the MIND Act aims to change by introducing harmonization through a federal channel. Elsewhere in Colorado, the passed House Bill 24-1058 [42] to protect neurodata under the CPA takes a strong stance to classify neurodata as sensitive information at state level. Sensitive information here is referred to as confidential data, taking a proactive approach against concerns of neurodata being misused [43]. The CPA did provide an exhaustive list of sensitive information, with neurodata now included as well. As part of the reform, consumer rights to process personal data are extended to relating to cognitive functions, as in neurodata as described by Farahany.

In the Latin American region, Mexico has also proposed multiple reforms, including Constitutional amendments. Instead of entrenching a specific right, the proposed change to Article 73 of the Mexico Constitution aims to allow state frameworks to protect against neurotechnology data [44]. Put more simply, Mexico sets the foundation for a potential framework of neurorights [45]. The themes in Mexico's amendment are similar to the AHRC's recently-published reports [2], [3], focusing on the need for informed consent and awareness of potential risks, cognitive liberty as part of personal integrity, and mental privacy. Mental privacy is also referred to as cognitive liberty and freedom of thought, which Mexico reiterating concern of potential neuromonitoring in the near-future, similar to neuromarketing. [44].

IV. THE NEED FOR NEUROTCH REFORM IN AUSTRALIA

Despite ongoing legal updates worldwide and domestic reports by the AHRC, Australia is yet to propose any formal reform. Importantly, not all the global reform is applicable to the Australian system. The Privacy Act is the main source for federal privacy protection in Australia for personal and sensitive information. In Section 6 of this legislation, "Personal information" is broadly defined as identifiable information about an identifiable person. In contrast, "Sensitive Information" provides an exhaustive list of information categories captured by the Privacy Act itself, somewhat similarly to Colorado. Health and biometric information are both included

as 'sensitive information', with the latter only protected if used for the purpose of biometric identification or automated verification [46]. Neurodata falls outside these two definitions as it is not biometric in nature. Nevertheless, the United Nations itself classifies neurodata as sensitive, a view supported by the AHRC. Consequently, there is a significant need for legal reform in Australia, particularly to ensure there is a balance between innovation and protection of data [10].

When considering what reform is needed for Australia, it is necessary to consider the factors outlined above as a bundle of rights. While it can appear that they are separate, individual parts that may need standalone reform like in Chile, Farahany stresses that they are part of a singular bundle of rights to be addressed. In Australian law, the concept of bundle of rights is a property law concept where smaller rights make up the whole 'bundle' or set of rights. [47].

V. PROPOSED FRAMEWORK

In order to solve the legislative and regulatory gap, this paper proposes the first of its kind Neurodata Privacy Protection Framework (NPPF). The framework is structurally similar to the APPs, but are a form of soft regulation (subject to being embedded in a statute like the Privacy Act and thus including hard penalties for breach) to provide organizations with additional guidance. Figure 1 demonstrates the NPPF neurodata governance structure around five interoperable pillars that enable enforceable, end-to-end trust from neurotechnology companies to the user.

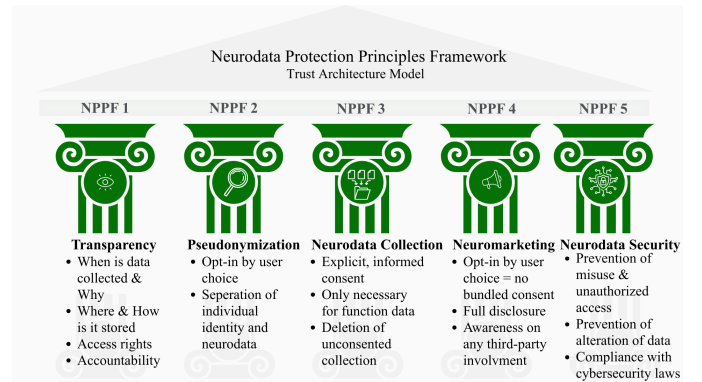


Fig. 1: Pillar-based Trust Architecture Model of NPPF for BCI highlighting key, foundational areas and principles of the framework

The NPPF achieves interoperability by adapting principles of open data management, disclosure, collection, and security of personal information. The framework is expected to be implemented by the Office of the Australian Information Commissioner [48], following Recommendation 3 in the AHRC final report [2].

Although the NPPF is primarily designed for the Australian system, it can be adapted to other jurisdictions as the core principles are echoed by scholars. When compared to constitutional and high-level general reforms, the NPPF demon-

strates to be a pragmatic, implementable model that embeds neurodata protections into existing privacy law, allowing for regulatory clarity as seen in Table I.

A. Neurodata Privacy Protection Framework

Guiding Principles:

- 1) **Mental Privacy** – protection as highly sensitive information;
- 2) **Informed Consent** – individuals must be made aware of what data are intended to be collected, for what purpose, and what the intended use will be. This allows for ethical use of data for marketing purposes, similarly to terms and conditions. Individuals also need to know the risks of the technology revealing unpredictable information;
- 3) **Non-discrimination on the Basis of Information** – neurodata must not be used to discriminate against an individual, in accordance with the suite of anti-discrimination laws;
- 4) **Information Security** – neurodata collected must be handled and stored in compliance with applicable cybersecurity laws.

NPPF 1: Transparent Neurodata Management: The object of this principle is to ensure that neurotechnology providers (manufacturers and organisations who utilise the technology for their employees or customers) manage neurodata in a transparent and ethical manner.

Neurotechnology providers must take reasonable steps to ensure that procedures and practices follow the NPPF Guiding Principles. Privacy policies must be updated to include neurodata-specific provisions where appropriate, including details of:

- a) circumstances where neurodata may be collected through the course of goods or services (depending on the nature of the provider);
- b) ways that the provider collects and holds neurodata;
- c) the purposes for which neurodata are collected and held;
- d) access channels for individuals seeking a copy of their neurodata or access to collected information;
- e) any risks that may be encountered during neurodata processing;
- f) disclosure conditions (including whether information may be shared with third parties);
- g) complaints mechanisms in the event of a breach or misuse of neurodata.

NPPF 2: Pseudonymization of Neurodata: Where possible, neurotechnology providers are to pseudonymize an individual's neurodata if the individual opts to do so. This principle is particularly relevant in research or commercial (neuromarketing) settings unless identification is necessary for the object of the endeavour. Whether pseudonymization is an option must be clearly communicated to the individual prior to data collection.

NPPF 3: Neurodata Collection: Neurodata must only be collected in the following circumstances:

- a) where an individual has explicitly consented to the collection of data, following informed consent principles.

Safeguards must be in place to ensure that individuals are fully aware of what they are consenting to; and

- b) where collection is necessary for the function of the neurotechnology and the provider's services or activities.

In the event that unconsented neurodata are obtained, the individual must be notified and provided with the option to access this data. The data must subsequently be deleted unless otherwise required by law.

NPPF 4: Neuromarketing: Providers must obtain informed, opt-in consent from individuals prior to using neurodata in neuromarketing. This is particularly important where neurodata may be disclosed to third parties for neuromarketing purposes. Individuals must be made fully aware of what this entails.

NPPF 5: Neurodata Security: Providers are required to take reasonable steps to ensure that neurodata are protected from:

- a) misuse;
- b) unauthorized access or disclosure to third parties;
- c) modification or alteration.

Relevant cybersecurity laws must be complied with given the digitised nature of neurodata, particularly for neurotechnologies relying on WiFi or Bluetooth connectivity.

VI. CASE STUDY SIMULATION UNDER THE NPPF FRAMEWORK

In order to test the validity of the proposed NPPF, it has been applied to a scenario where a case like *Girardi v Emotiv* took place in Australia. While legislative reform specifically to a section of the *Privacy Act 1988* would also be recommended for a stricter-legal approach, the NPPF would function similarly to the APPs. That is, guidelines attached to legislation that neurotechnology companies would need to follow to specifically safeguard their clients. The proposed NPPF is consistent with the underlying themes of cognitive autonomy in Mexico's constitutional amendments. Similarly, the NPPF operates nationally to ensure non-discrimination (NPPF 1, 2, 4), and brain privacy/cognitive liberty which the AHRC stressed [3].

In such a scenario, there would be a neurotechnology company (Fictional Inc) that collected Person A's neurodata during personal use of a BCI headset. The data was then collected beyond what Person A agreed to i.e. third-party marketing. Further, the data was not sufficiently pseudonymised, leaving Person A at risk of identification.

Under NPPF 1, Fictional Inc would be obligated to clearly disclose at what point the neurodata is collected, such as raw electroencephalogram (EEG) data, as well as any secondary uses of this data. It extends to transparency of what purposes the data is collected for, who will see the data, and where it will be stored. Unlike the legislation in *Girardi v Emotiv*, the NPPF's neurodata-specific policy and explicit language make it unlikely that Fictional Inc would violate it in the first instance. In the event that they do, the fact that it is a neurodata-specific legislation allows the courts to have a streamlined case without the need for extraneous expert

	NPPF	Colorado Privacy Act Amendment	US MIND Act	Chile Neurorights Amendment	Mexico Neurorights Reform
Summary	Requires informed consent, opt-in pseudonymization, opt-in neuromarketing, and security duties for neurodata collection and processing.	Expands the definition of sensitive data to include neural data within the general consumer privacy regime.	Takes a policy-focused approach to neurodata governance.	Entrenches neurorights constitutionally through a reform package including general law and constitutional amendments.	Introduces a neurorights-focused reform package including general law and constitutional amendments.
Areas Covered	Covers consumer and workplace use, permitted practices, and consequences for misuse.	Covers consumer privacy complaints and recognizes neurodata as sensitive data under existing protections.	Covers education on neurodata misuse and possible harmonization of neurodata standards in the United States.	Protects neurodata and neurotechnology use, with broad emphasis on mental privacy and cognitive liberty.	Addresses cognitive liberty, consent, and equitable access, while highlighting concern about neurodata misuse.
Gaps	Does not include an explicit penalties regime; this would depend on the legislation used to implement it.	Is not neurotechnology-specific and gives limited clarity on neuromarketing or pseudonymization penalties.	Does not focus on helping neurotechnology providers with regulatory compliance.	Uses context-specific constitutional language and may face vagueness in enforcement.	Is broad in scope and depends on multiple departments for implementation.
Overall Relevance for Australia	Fits well with the APP-based Australian framework and could be enforced through OAIC powers.	Helps as a model for classifying sensitive data, but aligns less closely with the APP approach.	Provides useful comparative policy context.	Is not a practical immediate pathway for Australia, but helps frame the normative basis of the NPPF.	Its constitutional focus is less directly transferable, but its themes may still inform NPPF principles.

TABLE I: Comparative overview of neurodata and neurorights frameworks

evidence. NPPF 3 works seamlessly with this by requiring consent for any type of data collection. Any use against what Person A consented to creates a clear breach, meaning Fictional Inc would be clearly aware of the practices not to engage in.

If Fictional Inc failed to disclose the third-party marketing use, they would also be going against NPPF 4 which requires explicit consent specifically for neuromarketing purposes. Contrary to the court’s decision in *Girardi v Emotiv*, neuromarketing is not banned under the framework, but rather legitimized with the need for consent. NPPF 4 looks to Mexico’s themes of informed consent and personal integrity, which is violated if Fictional Inc acts inconsistently with the guidelines.

Under NPPF 2, even if Fictional Inc disclosed the third-party data use, they are required to take all steps reasonable and proportionate to minimize identification if a user opts for it. A failure to do so with specific instructions from the user evidence harm to Person A’s data.

NPPF 5 would be most relevant if Fictional Inc’s data storage would be subject to a cybersecurity breach, a concern which the Court raised in *Girardi v Emotiv*. Under these circumstances, Fictional Inc would be required to demonstrate reasonable steps to protect data during collection ie use, and storage. A failure to do so may invoke penalties under relevant cybersecurity laws.

Overall, the NPPF has been designed to be clear in its’ language and cover the key concerns of *Girardi v Emotiv*, industry scholars, and other jurisdictions (namely US and Latin America more broadly). It ensures that companies are clearly aware of the practices not to engage in, reducing the likelihood of litigation. In relation to similarity, while the NPPF differs vastly from Chile’s legal position even pre-*Girardi v Emotiv*, the decision of the case would be the same

in holding Emotiv accountable. Importantly, the outcome does depend on whether they would comply with each of the NPPF principles. However, despite benefits, there are limitations in the NPPF enforcement, demonstrated in Table I, as it largely depends on which legislation it is embedded within. Further, as with the APPs, frameworks as subject to exceptions and are more of a soft-law approach rather than a hard statute itself with concrete penalties. These limitations can however be complimented by an amendment to the *Privacy Act 1988* itself, similarly to Colorado, to ensure that there is a hard avenue for enforcement.

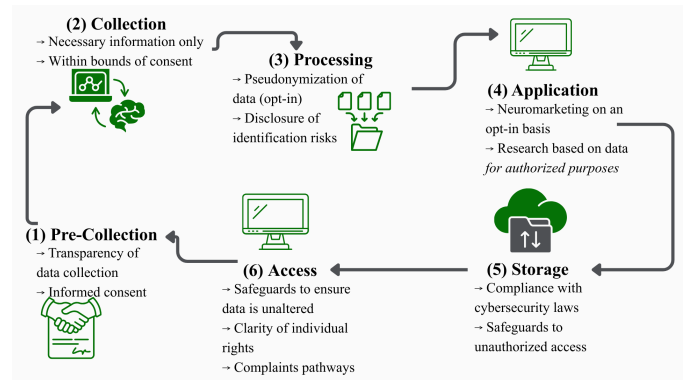


Fig. 2: NPPF Integration to BCI Lifecycle

Fundamentally, it is drafted in the spirit of the APPs and with the Australian legal system in mind, though there is room for discussion and collaboration to apply it to other countries and systems. Figure 2 highlights the way the NPPF is fully integratable across the BCI lifecycle, ensuring that neurodata protection is practically applied continuously from design, data collection and feedback loops.

VII. CONCLUSION

With the increasing uptake of neurotechnology, there comes increasing concerns at a global level on how companies are handling the neurodata. Neurodata is a complex, sensitive piece of data and the privacy risks extend beyond handling and into cybersecurity, pseudonymization and even economic benefit. However, despite it being a practical reality recognized by major market players like the US, and jurisdictions in South America, it is evident that Australia also needs to bridge the gap and implement safeguards. While technology can be loosely captured by the TGA legislations, Australian privacy laws have been demonstrated not to be up to date with the specific nature of neurodata. In addition to an amendment of the *Privacy Act 1988* itself, there is a clear need to implement the NPPF to ensure that Australians have the same protections that the APPs provide to personal, sensitive information for neurodata. Furthermore, there is scope for the NPPF to be adapted to other jurisdictions where it may be used as soft-law or hard law like Mexico's general law reforms.

REFERENCES

- [1] A. Keutayeva, C. J. Nwachukwu, M. Alaran, Z. Oturbay, and B. Abibulaev, "Neurotechnology in gaming: A systematic review of visual evoked potential-based brain-computer interfaces," *IEEE Access*, 2025.
- [2] A. H. R. Commission, "Peace of mind: Navigating the ethical frontiers of neurotechnology and human rights," report, Australian Human Rights Commission, October 2025.
- [3] Australian Human Rights Commission, "Protecting cognition: Background paper on neurotechnology and human rights," background paper, Australian Human Rights Commission, Sydney, NSW, Australia, March 2024.
- [4] A. Nouri, "A scoping review of educational neurotechnology: Methods, applications, opportunities, and challenges," *Review of Education*, vol. 13, no. 2, p. e70070, 2025.
- [5] I. C. Office, "Tech futures: Neurotechnology," report, Information Commissioner's Office, June 2023.
- [6] K. M. Patrick-Krueger, I. Burkhart, and J. L. Contreras-Vidal, "The state of clinical trials of implantable brain-computer interfaces," *Nature reviews bioengineering*, vol. 3, no. 1, pp. 50–67, 2025.
- [7] T. Istace and M. Costas Trascasas, "Between science-fact and science-fiction innovation and ethics in neurotechnology," *The Geneva Academy of International Humanitarian Law and Human Rights*, no. May, 2024.
- [8] Q. Deng, Z. Fu, N. Ma, and B. Wang, "Application and future directions of brain-computer interfaces in neurological disorders: technological advances, clinical practices, and challenges," *Brain Hemorrhages*, 2025.
- [9] M. H. Maghami, A. M. Sodagar, A. Lashay, H. Riazzi-Esfahani, and M. Riazzi-Esfahani, "Visual prostheses: The enabling technology to give sight to the blind," *Journal of ophthalmic & vision research*, vol. 9, no. 4, p. 494, 2014.
- [10] P. Magee, M. Ienca, and N. Farahany, "Beyond neural data: Cognitive biometrics and mental privacy," *Neuron*, vol. 112, no. 18, pp. 3017–3028, 2024.
- [11] P. Kellmeyer, "Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices," *Neuroethics*, vol. 14, no. 1, pp. 83–98, 2021.
- [12] D. Hallinan, P. Schutz, M. Friedewald, and P. De Hert, "Neurodata and neuroprivacy: Data protection outdated?," *Surveillance & Society*, vol. 12, no. 1, pp. 55–72, 2014.
- [13] N. A. Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*. St. Martin's Press, 2023.
- [14] K. M. Talha, "Closing remarks by h.e. mr khondker m. talha, president of the 43rd session of the general conference of unesco." 43rd Session of the General Conference of UNESCO, Samarkand, Uzbekistan, Nov. 2025. Programme and meeting document, document code GBS-43-PGC-2025-03, 6 pages.
- [15] N. A. Limited, "Neurotech interactive charts." Web tool, n.d.
- [16] A. Sigov, L. Ratkin, L. A. Ivanov, and L. D. Xu, "Emerging enabling technologies for industry 4.0 and beyond," *Information Systems Frontiers*, vol. 26, no. 5, pp. 1585–1595, 2024.
- [17] K. Badgi and T. Rajic, "When thought becomes data: The mind act and the coming debate over neurotechnology." Analysis published by the Center for Strategic and International Studies (CSIS), November 4 2025.
- [18] T. G. Administration, "Clarifying and strengthening the regulation of medical device software including artificial intelligence (ai)," consultation report, Therapeutic Goods Administration, Australian Government, 2025.
- [19] C. of Australia, "Privacy act 1988 (cth) — latest consolidated version." <https://www.legislation.gov.au/C2004A03712/latest/text, 1988>.
- [20] Commonwealth of Australia, "Privacy act 1988 (cth), schedule 1 — australian privacy principles." https://classic.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html, 1988.
- [21] O. of the Australian Information Commissioner, "History of the privacy act." Web page, n.d.
- [22] "International covenant on civil and political rights." <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, 1966>. Adopted 16 December 1966, entered into force 23 March 1976; UN General Assembly resolution 2200A (XXI).
- [23] D. Lindsay, "An exploration of the conceptual basis of privacy and the implications for the future of australian privacy law," *Melbourne University Law Review*, vol. 29, no. 1, pp. 131–178, 2005.
- [24] "Australian information commissioner act 2010 (cth)." Commonwealth Act, 2010.
- [25] "Privacy amendment (notifiable data breaches) act 2017 (cth)." Commonwealth Act, 2017.
- [26] O. of the Australian Information Commissioner, "Statutory tort for serious invasions of privacy." Web page, June 19 2025.
- [27] "Kurraaba group Pty Ltd & Anor v Williams [2025] NSWDC 396." Decision of the New South Wales District Court, 2025.
- [28] T. Ginsburg and J. Melton, "Does the constitutional amendment rule matter at all? amendment cultures and the challenges of measuring amendment difficulty," *International Journal of Constitutional Law*, vol. 13, no. 3, pp. 686–713, 2015.
- [29] B. C. Newell, N. Purtova, Y. E. Moon, and H. J. Paterson III, "Regulating the data market: The material scope of american consumer data privacy law," *U. Pa. J. Int'l L.*, vol. 45, p. 1055, 2023.
- [30] H. Yang and L. Jiang, "Regulating neural data processing in the age of bcis: Ethical concerns and legal approaches," *Digital Health*, vol. 11, p. 20552076251326123, 2025.
- [31] H. C. Oyarzún and M. U. Conejeros, "La protección de datos personales tras la ley 21.719: Implicancias regulatorias y proyecciones para las empresas en las relaciones laborales," *Revista de Derecho Aplicado LLM UC*, no. 15, 2025.
- [32] E. Union, "Recital 26: Not applicable to anonymous data." <https://gdpr-info.eu/recitals/no-26/, 2016>.
- [33] M. Ienca and R. Andorno, "Towards new human rights in the age of neuroscience and neurotechnology," *Life sciences, society and policy*, vol. 13, no. 1, p. 5, 2017.
- [34] J. G. Browning, "Are technology and the law on the same" wave-length"?: Examining the new frontier of brainwaves and data privacy," *NCJL & Tech.*, vol. 26, p. 345, 2024.
- [35] S. Lighthart, M. Ienca, G. Meynen, F. Molnar-Gabor, R. Andorno, C. Bublitz, P. Catley, L. Claydon, T. Douglas, N. Farahany, et al., "Mind-ing rights: Mapping ethical and legal foundations of 'neurorights'," *Cambridge quarterly of healthcare ethics*, vol. 32, no. 4, pp. 461–481, 2023.
- [36] A. Kübler and N. Birbaumer, "Brain-computer interfaces and communication in paralysis: Extinction of goal directed thinking in completely paralysed patients?," *Clinical neurophysiology*, vol. 119, no. 11, pp. 2658–2666, 2008.
- [37] L. Szoszkiewicz and R. Yuste, "Mental privacy navigating risks, rights and regulation advances in neuroscience challenge contemporary legal frameworks to protect mental privacy," *EMBO reports*, pp. 1–5, 2025.
- [38] J. C. Bublitz, "Novel neurorights: from nonsense to substance," *Neuroethics*, vol. 15, no. 1, p. 7, 2022.
- [39] L. Maderthaner and M. J. Edwards, "Mind-body integration in brain health," *Clinical and Translational Neuroscience*, vol. 9, no. 3, p. 37, 2025.

- [40] T. Denison and M. J. Morrell, “Neuromodulation in 2035: the neurology future forecasting series,” *Neurology*, vol. 98, no. 2, pp. 65–72, 2022.
- [41] United States Congress, “Management of individuals’ neural data act of 2025 (s.2925).” <https://www.congress.gov/bill/119th-congress/senate-bill/2925/text>, 2025. Introduced bill directing the Federal Trade Commission to conduct a study on the governance of neural data and related data.
- [42] Colorado General Assembly, “House bill 24-1058: Protect privacy of biological data.” <https://leg.colorado.gov/bills/hb24-1058>, 2024. Amends the Colorado Privacy Act to include neural data as sensitive personal data; effective August 7, 2024.
- [43] “Second regular session, seventy-fourth general assembly.” Colorado General Assembly, 2024–2025.
- [44] L. L. Senado de la República, H. Congreso de la Unión, “Iniciativa con proyecto de decreto que reforma el artículo 73 de la constitución política de los estados unidos mexicanos.” Legislative proposal document, September 26 2023.
- [45] S. de la República, “Iniciativa que expide la ley general de neuroderechos y neurotecnologías,” jul 2024. Legislative initiative introducing a general framework for neurorights and neurotechnologies in Mexico; original bill text available as PDF attachment.
- [46] “Privacy act 1988 (cth) s 6(d)–(e).” Commonwealth Act, 1988.
- [47] A. L. R. Commission, “Definitions of property,” in *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws*, no. 129 in ALRC Report, ch. 18, Australian Law Reform Commission, 2016.
- [48] O. of the Australian Information Commissioner, “Australian privacy principles guidelines.” <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>, 2024.