Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 139

Neurotechnology and Privacy: A Comparative Analysis of US and EU Approaches

Elif Kiesow Cortez

2025

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Dr. Elif Kiesow Cortez has worked in policy advisory, project management, and academic roles on the governance of emerging technologies. Elif collaborates in a research project with the Stanford Institute for Human-Centered Artificial Intelligence. Elif has been appointed as an advisory board member for projects of leading institutions including the UNFCCC, IAPP, and European Research Council. She has also founded and led the AI & LegalTech Lab. Previously, Elif was a John M. Olin Fellow in Law and Economics at Harvard Law School. Her doctoral research at the Institute of Law and Economics, University of Hamburg, Germany, was funded by the German Research Association (DFG). During her doctoral studies, she was a visiting researcher at Harvard Business School and Berkeley School of Law. Elif is an expert on behavioral strategies for effective tech policies addressing cooperation problems between public and private actors. Elif has acquired research grants for projects on tech governance commissioned by the Dutch Research Council (NWO) and the US National Science Foundation (NSF). Elif has been a TTLF Affiliate since 2020.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Elif Kiesow Cortez, Neurotechnology and Privacy: A Comparative Analysis of US and EU Approaches, Stanford-Vienna TTLF Working Paper No. 139, http://ttlf.stanford.edu.

Copyright

Abstract

As neurotechnology advances rapidly, the integration of brain-computer interfaces, neural data collection, and cognitive enhancement tools is raising complex ethical and legal challenges, particularly concerning individual privacy. This paper presents a comparative analysis of how the United States and the European Union approach the regulation of neurotechnology with respect to privacy protection. Drawing on legal frameworks, policy developments, and recent case studies, we examine the extent to which each jurisdiction addresses the unique nature of neural data, including its sensitivity, potential for misuse, and implications for cognitive liberty. Our analysis on the EU focuses on the General Data Protection Regulation (GDPR), which is applicable across all EU member states. For the U.S. framework, it will focus on potential privacy protections under three state legislations which include a definition for "neural data", the Colorado Privacy Act (CPA), the California Consumer Privacy Act (CCPA), and the Montana Genetic Information Privacy Act (GIPA). Our analysis aims to highlight key issues, risks, and potential avenues for harmonization. The paper concludes by offering recommendations for future transatlantic policy development that balances innovation in neurotechnology with robust privacy safeguards.

Table of Contents

I. Introduction

Neurotechnologies, which allow brain activity to be recorded, analyzed, and manipulated, have moved beyond their original clinical applications. They are increasingly marketed as consumer-grade devices available to healthy populations for cognitive or physical enhancement in work, education, and entertainment settings, often without expert supervision.[1]

As these systems mature, they carry promises such as new therapies for neurological diseases, or new modes of human–computer interaction. They also carry new risks as neural data and brain-directed stimulation implicate the private sphere of thought and intention, and might raise questions that existing privacy and consumer-protection regimes were not built to answer. This article surveys that landscape with a focus on commercial applications and the privacy issues they provoke, comparing emerging responses in the United States and the European Union and situating them within an international debate about neurorights and privacy.

Current efforts to govern the neurotech space include regulatory efforts on both sides of the Atlantic, such as the Colorado Privacy Act (CPA), California Consumer Privacy Act (CCPA), and Montana Genetic Information Privacy Act (GIPA), laws including neuro data as a special category of data in privacy legislation, as well as the EU's GDPR and AI Act. The subject also received attention by international players such as UNESCO and OECD,

[1] European Parliament. Directorate General for Parliamentary Research Services., *The Protection of Mental Privacy in the Area of Neuroscience: Societal, Legal and Ethical Challenges*. (Publications Office 2024) <https://data.europa.eu/doi/10.2861/869928> accessed 30 September 2025.

in addition to already codified laws, for example from Chile including neurorights in their national legal system during the latest constitutional reform.[2] These efforts are shaped also in light of the scholarly discussions on this important issue. Some key literature includes work focusing on neurorights[3] where scholars define human rights issues associated with neurotechnology starting with accessing an individual's mental states, inferring the associated behaviors and/or opinions with those mental states and the risk of interfering with these mental states.

Neurotechnology tools can encompass devices that can monitor brain activity as well as those that can intervene into brain activity in addition to bimodal devices with capacity to do both.[4] Devices that once merely "read" brain signals now also "write" to the brain; platforms that began as wellness gadgets are integrating AI models that draw deeper inferences from the same raw data; and medical and consumer markets are converging through mobile apps and cloud services.[5] The result is a fast-evolving ecosystem in which data flows, device capabilities, and business models cross traditional regulatory lines.

Neural data can expose information of unusual sensitivity: emotional states, recognition of stimuli, even tentative inferences about memories or preferences, and these inferences can be drawn from signals that might be perceived as "low risk" at the moment of collection, making informed consent more fragile. As a result, what might appear to be

[2] Sergio Ruiz and others, 'Neurorights in the Constitution: From Neurotechnology to Ethics and Politics' (2024) 379 Philosophical Transactions of the Royal Society B: Biological Sciences 20230098.
[3] Sjors Ligthart and others, 'Minding Rights: Mapping Ethical and Legal Foundations of "Neurorights"' (2023) 32 Cambridge Quarterly of Healthcare Ethics 461.
[4] ibid.
[5] Genser, Jared, Damianos, Stephen and Yuste, Rafael, 'Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies' (Neurorights Foundation 2024).

mere focus tracking today may support complex profiling practices tomorrow. Cybersecurity of the collected or inferred data also adds another layer of concern on mental integrity itself. In the face of these emerging technological possibilities in the neurotech field, this article will bring attention to the three key concepts of mental integrity, mental privacy and cognitive liberty and explores in what ways they are being reflected in relevant legislation.[6]

Rising awareness of the advance of neurotech has attracted the attention of experts and policymakers to assess potential risks and implications as well as the adequacy of regulatory regimes to govern these. For instance, across Europe, the Council of Europe and the EU have issued expert reports on neurotechnology, yet no dedicated laws have followed. Scholars have argued that Article 8 of the European Charter of Fundamental Rights, dedicated to protection of personal data, already provides an extensive recognition and protection of neurodata.[7] This is largely because the GDPR's privacy framework, with its broad definitions of sensitive data and strong enforcement tools, already covers neural data more effectively than many other regions. Even so, the regulation predates the rise of neurotechnology, and the question of whether it should apply to this field continues to spark debate.[8]

The remainder of the introduction section will provide a brief overview of the neurotech field and applications. The article will then explore in Section II the various potential

[6] Ligthart and others (n 3).
[7] Timo Istace, 'Protecting the Mental Realm: What Does Human Rights Law Bring to the Table?' (2023) 41 Netherlands Quarterly of Human Rights 214.
[8] Łukasz Szoszkiewicz and Rafael Yuste, 'Mental Privacy: Navigating Risks, Rights and Regulation' (2025) 26 EMBO Reports 3469.

privacy implications of this rapidly advancing technology. The ensuing two sections will discuss legal frameworks that could be applied to govern privacy aspects of neurotech on both sides of the Atlantic, namely state level laws in the US case (Section III) and EU legislation in Europe (Section IV). This is followed by an exploration of ethical principles that could inform and underpin future EU-US coordination efforts to govern privacy risks related to neurotech (Section V). The conclusion recapitulates some of the main points and offers further tentative recommendations.

1. Neurotechnology: Commercial Applications

According to 2025 draft recommendations by UNESCO, neurotechnology refers to tools that measure and analyze physical, chemical, or biological signals from the nervous system, that can record, predict, or monitor neural activity, aid diagnosis, or control external devices such as brain–computer interfaces, sometimes providing real-time feedback with stimulation or inhibition.[9][10]

[9] The draft recommendations use the following definitions under the section "Scope and Definition": *"(a) Technical tools that measure and analyse physical (e.g. acoustic, electrical, optical, magnetic and/or mechanical), chemical and biological signals associated with the structure of and functional signals from the nervous system (including cell therapy and gene therapy). These may be used to identify, record, predict and/or monitor properties of nervous system activity, understand how the nervous system works, diagnose pathological conditions, or control external devices (brain machine interfaces (BMI), often referred to as brain computer interfaces (BCI))…. (b) Technical or interventional tools that interact with the structure or functions of the nervous system to change its activity, for example, to restore sensory input, such as hearing (e.g. cochlear implants) or deep brain stimulation (DBS). They are meant to modulate the functions of the nervous system, send signals directly to the nervous system by applying acoustic, electrical, magnetic, ultrasound or optical stimulation…"*

[10] UNESCO, 'Draft Recommendation on the Ethics of Neurotechnology - UNESCO Digital Library' (2025) <https://unesdoc.unesco.org/ark:/48223/pf0000394866> accessed 30 September 2025.

Now, exemplary technical tools will be presented with an emphasis on their potential use and derived risks.

2. Brain-Computer Interfaces

A Brain-Computer Interface (BCI) is a technology that lets the brain communicate directly with machines. Some are invasive, using implanted electrodes to capture brain signals at very high resolution, while others are non-invasive, like electroencephalography (EEG) headsets that sit on the scalp. Invasive BCIs have achieved striking results, such as helping ALS patients "type" by thought or enabling people with paralysis to move robotic arms.[1112] Non-invasive versions are safer but less precise, often sold as consumer gadgets for boosting focus or playing video games with brain signals.[13] BCIs can either "read" brain activity to interpret a person's intentions or "write" signals back into the brain to alter its activity. The most advanced designs do both, which opens exciting possibilities but also serious risks, such as the danger of outside interference with autonomous choices.[14]

[11] K Michelle Patrick-Krueger, Ian Burkhart and Jose L Contreras-Vidal, 'The State of Clinical Trials of Implantable Brain–Computer Interfaces' (2025) 3 Nature Reviews Bioengineering 50.
[12] Niels Birbaumer, 'Breaking the Silence: Brain-Computer Interfaces (BCI) for Communication and Motor Control' (2006) 43 Psychophysiology 517.
[13] Nita Farahany, 'The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology' [2023] Faculty Books.
[14] Paheenthararajah, Kokularajah and Martens, Julia, 'Ethical and Legal Challenges of Neurotech' (*DLA Piper*, 27 March 2025) <https://www.dlapiper.com/en/insights/publications/2025/03/ethical-and-legal-challenges-of-neurotech> accessed 30 September 2025.

3. Neuroimaging and Neurosensing

Methods like functional MRI (fMRI), electroencephalography (EEG), magnetoencephalography (MEG) with their capabilities for detecting and mapping brain activity, and newer portable brain scanners let scientists, and increasingly companies, track brain activity and even make inferences about thoughts, intentions, or recognition. Studies using fMRI, for instance, have predicted simple decisions before they are made and revealed when someone recognizes a familiar image. This ability has been repurposed for marketing: neuromarketing firms use brain scans to test ads or products, tapping into subconscious reactions that people may not realize they have. Large corporations already employ such techniques, often using EEG or fMRI, in what some describe as "mind mining." Once limited to research labs and clinical settings, these tools are now appearing in consumer products like wellness headsets, prompting scholars to label them "pervasive neurotechnology."[15]

4. Neuromodulation and Neurostimulation

These are technologies designed to actively stimulate the brain or nervous system in order to change its activity. They include invasive medical devices such as Deep Brain Stimulation (DBS) implants, which deliver targeted electrical pulses to treat conditions like Parkinson's disease, essential tremor, or severe depression. Non-invasive approaches, such as transcranial magnetic stimulation (TMS) and transcranial direct

[15] Marcello Ienca and Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotechnology' (2017) 13 Life Sciences, Society and Policy 5.

current stimulation (tDCS), can alter neural activity through the skull and are being studied for applications ranging from mood regulation to cognitive enhancement. However, these “write-in” technologies raise unique concerns regarding safety and personal autonomy. For example, a device could, whether intentionally or through hacking, influence an individual’s emotions or behavior. While invasive systems are subject to strict medical oversight, many consumer-oriented non-invasive stimulators, marketed for wellness or entertainment, have historically faced little regulation, prompting growing attention from policymakers.[16]

5. Emerging Consumer Neurotech

A growing array of consumer neurotechnology devices has entered the market, ranging from EEG-based headbands and earbuds marketed for stress reduction or meditation to neural input systems designed for gaming and virtual reality. These products often integrate with smartphone applications and cloud platforms, meaning brain-signal data is collected outside of medical or research contexts.[17] While such devices usually capture relatively simple neural indicators, such as attention levels or sleep stages, advances in AI raise concerns that the same data could eventually be used to extract far more detailed insights. A headset that today measures focus might, in the near future, enable algorithms to infer emotional states or even political preferences, a prospect

[16] Paheentharajah, Kokularajah and Martens, Julia (n 14).
[17] Szoszkiewicz and Yuste (n 8).

made plausible by recent research using fMRI and AI to reconstruct perceived images and speech.

All in all, neurotechnology today covers everything from medical implants that change lives to consumer apps and marketing tools. The field is growing at an extraordinary pace: investments rose more than 700% between 2014 and 2021, reaching $33 billion, and around 1,400 companies are now working in the sector, with most based in the U.S. and Europe.[18] This rapid growth highlights the pressing need to address ethical and privacy concerns. As neurotech shifts from clinical settings into mainstream markets, it raises urgent questions about who controls, accesses, and benefits from brain data, the digital footprints of our neural activity. In the next section a series of privacy-related issues raised by these neurotech advances will be explored in more detail.

II. Privacy Implications of Neurotechnology

Neurotechnology presents what many call the *last frontier* of privacy. Unlike other forms of personal information, data derived from brain activity, often called *neural* or *brain data*, is uniquely sensitive. It has the potential to not only reveal what we do, but also why we do it; not just our actions, but our hidden thoughts, feelings, and intentions. Scholars and ethicists emphasize that, this blurs the line between personal information and the human thought[19], while increasing the importance of protection of personal data and

[18] 'Ethics of Neurotechnology | UNESCO' <https://www.unesco.org/en/ethics-neurotech> accessed 30 September 2025.
[19] Szoszkiewicz and Yuste (n 8).

intertwining it with discussing freedom of thought. From this uniqueness flow a series of distinct privacy and ethical concerns: questions about mental privacy and free will[20], the depth of personal information that neural data can expose, the dangers of hacking or manipulation, challenges to informed consent, and even the possibility of self-incrimination through brain evidence in court.

The rapid proliferation of consumer neurotech is therefore outstripping existing governance and oversight frameworks in the US, leading to creation of new protections for consumers at the state level, outside the regulated healthcare domain.[21] In the EU, the debate also continues over whether existing EU rights frameworks already provide sufficient protection. Introducing new rights may inadvertently restrict established ones or create legal gaps, especially given the lack of case law. Instead, the report recommends strengthening regulation through targeted measures, such as risk assessments aligned with the AI Act, improved public communication, funding for research, support for EU-based providers, and evaluating whether new technical standards are needed, to safeguard individuals while fostering responsible innovation.[22]

[20] European Parliament. Directorate General for Parliamentary Research Services., *The Protection of Mental Privacy in the Area of Neuroscience: Societal, Legal and Ethical Challenges*. (Publications Office 2024) <https://data.europa.eu/doi/10.2861/869928> accessed 30 September 2025.
[21] 'States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News' (16 July 2025) <https://www.cbsnews.com/news/state-privacy-laws-brain-data-devices/> accessed 30 September 2025.
[22] European Parliament. Directorate General for Parliamentary Research Services. (n 18).

1. Mental Privacy and Cognitive Liberty

Mental privacy refers to the right to keep one's thoughts, feelings, and brain states free from unwanted intrusion or disclosure. It is closely tied to what some call *cognitive liberty*, the right to freedom of thought and control over one's own mental processes. Historically, freedom of thought has been considered absolute and inviolable, no government or entity should force you to reveal or change your inner thoughts. Neurotechnology challenges this by creating the possibility of *accessing* thoughts or influencing them. For example, if an EEG device can infer whether a person recognizes a certain image or whether they are paying attention, using that data without consent could violate mental privacy. Likewise, if a "brain stimulation" gadget could unknowingly shape a user's decisions, it would infringe on cognitive liberty. These concerns have led ethicists to argue for explicit rights to mental privacy, mental integrity, and cognitive freedom in the era of neurotech.[23]

2. Sensitive Data

Neural data can expose information of extraordinary sensitivity. Under the GDPR, sensitive personal data is formally referred to as "special categories of personal data" and the definition of it includes data on political opinions, data concerning health or a person's sexual orientation. High-resolution brain scans or invasive recordings might expose one's emotional reactions, sexual orientation, political ideology, or propensity for

[23] Ligthart and others (n 2).

certain behaviors.[24] Even simpler EEG signals, when analyzed with sophisticated algorithms, have been shown to infer things like a person's visual memories or words they are thinking of and therefore goes far beyond typical personal data like one's heart rate or location history. As a result, the potential misuse is correspondingly alarming, imagine a company using subtle brain signals to determine your unspoken preferences and manipulating advertisements accordingly, or an authoritarian regime surveilling citizens for "undesirable" thoughts. UNESCO warns about a wide array of possible misuses ranging from implications for consumer rights, e.g. in that companies "can influence customers' behavior for profit maximization..."[25] to broader societal challenges when "threatening our democracies and the foundations of society"[26] as a result of exploitation of neural data from consumer devices.

3. Cybersecurity Risks

Privacy is also threatened by the security vulnerabilities of neural data. Like any digital information, brain signals can be intercepted, hacked, or manipulated. Researchers have even conceptualized "brain spyware,"[27] malicious code capable of extracting neural information or inserting signals without awareness. A compromised wireless BCI could not only leak brain data but also deliver unauthorized stimulation, violating both privacy and mental integrity. A breach of a neurotech database, containing raw EEG recordings,

[24] Szoszkiewicz and Yuste (n 8).
[25] 'Ethics of Neurotechnology | UNESCO' (n 18).
[26] ibid.
[27] Marcello Ienca and Pim Haselager, 'Hacking the Brain: Brain–Computer Interfacing Technology and the Ethics of Neurosecurity' (2016) 18 Ethics and Information Technology 117.

would thus be even more invasive than a health record leak. Experts stress the need for rigorous cybersecurity standards and *privacy by design* in all neurotechnology systems.

4. Informed Consent

Conventional privacy law often relies on consent, but neurotechnology complicates this safeguard. Users cannot easily predict what today's neural data might reveal in the future, as analytic techniques rapidly advance. A dataset collected for "focus tracking" today could later expose emotional patterns or memories, undermining meaningful consent.[28] Voluntary consent is also questionable in power-imbalanced contexts, such as workplaces or schools, where refusing to wear a neurodevice may not be a real option. Consumer neurotech practices often lag behind: a single app agreement may authorize continuous, granular collection with little user control. Scholars argue for new models of consent, such as session-by-session permissions and easy pause/delete options, tailored to neural data.[29]

5. Self-Incrimination

A further concern arises in law enforcement and courts on that neurodata could be potentially used to compel testimony, violating the right against self-incrimination.[30] For

[28] 'States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News' (n 21).
[29] Szoszkiewicz and Yuste (n 8).
[30] Nita A Farahany, 'Incriminating Thoughts' (2012) 64 Stanford Law Review 351.

example, requiring a suspect to undergo an fMRI lie-detection or EEG "brain fingerprinting" test may be equivalent to forcing them to disclose their thoughts[31] and scholars urge proactive safeguards.[32]

III. Legal Frameworks in the United States

In the United States, privacy law has long been characterized by a sectoral and reactive orientation rather than a unified, comprehensive federal framework. Protections have typically been tied to particular categories of information (e.g., health, financial, or educational records) or specific practices (such as video rentals or telephone records). Within this patchwork system, "brain data" historically occupied a legal gray zone. Neural information collected in medical contexts, such as an EEG performed in a hospital, fell under the scope of the Health Insurance Portability and Accountability Act (HIPAA). By contrast, the identical data gathered by consumer-oriented EEG headsets or wellness applications was not protected by HIPAA, as the companies producing these devices were not recognized as "covered entities." Moreover, unlike fingerprints or DNA, brainwave data were not classified as biometric identifiers under most U.S. laws, including Illinois's pioneering Biometric Information Privacy Act. For many years, cognitive data gathered by private technology firms was therefore largely unregulated, governed only by general consumer protection law or the companies' own privacy policies.

[31] Emily RD Murphy and Jesse Rissman, 'Evidence of Memory from Brain Data' (2020) 7 Journal of Law and the Biosciences lsaa078.
[32] European Parliament. Directorate General for Parliamentary Research Services. (n 18).

This regulatory lacuna has been underscored by empirical findings. A 2024 investigation[33] of 30 consumer neurotechnology companies revealed that 29 had unfettered access to users' neural data and imposed no meaningful restrictions on that access. Almost all companies permitted third-party data sharing, often without explicitly referencing "brain data" in user agreements or adequately informing users of the sensitivity of such information. Effectively, users who accepted boilerplate privacy policies authorized companies to collect, process, and commercialize their cognitive data with little recourse. As consumer neurotechnologies proliferated, spanning meditation headbands, smart earbuds, and even workplace monitoring tools, advocates and policymakers began to sound alarms over the absence of regulatory oversight.

1. Emerging State Legislation on Neural Data

Beginning around 2022, state legislators initiated efforts to address these regulatory gaps by introducing statutes specifically targeting neural data privacy. By mid-2025, Colorado[34], California[35], and Montana[36] had enacted pioneering laws explicitly identifying "neural data" or "brain data" as protected information. While varying in detail, these laws share several core features. It is important to note that these references and definitions

[33] Genser, Jared, Damianos, Stephen and Yuste, Rafael (n 5).
[34] Colorado House Bill 24-1058 An act concerning protecting the privacy of individuals' biological data, and, in connection therewith, protecting the privacy of neural data and expanding the scope of the 'Colorado Privacy Act' accordingly [HB24-1058].
[35] California SB 1223 An act to amend Section 1798.140 of the Civil Code, relating to privacy [SB 1223].
[36] Montana SB 163 An act revising the genetic information privacy act; including neurotechnology data in the scope of the genetic information privacy act [SB163].

on neural data were included via amending the respective broader privacy acts in Colorado and California (Colorado Privacy Act and California Consumer Privacy Act), while in Montana the amendment concerned the "Genetic Information Privacy Act".

A. Definition of neural data

The statutes adopt expansive definitions of neural data, typically encompassing both raw outputs (e.g., EEG signals, brain scans) and derivative inferences about mental states, such as emotions, attention, or fatigue. This reflects recognition that even apparently "basic" neural signals, when analyzed with advanced algorithms, can yield highly sensitive insights.[37]

Colorado's HB 24-1058 amends the CPA, to include biological data and neural data. As per the proposed definition biological data also includes "data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily function…" and the more specific neural data corresponds to "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device".

[37] Farahany (n 13).

California's SB 1223 takes a similar approach to Colorado and includes neural data under sensitive personal information while defining it more narrowly than Colorado by excluding data that is inferred from nonneural information. SB 1223 defines neural data to mean "information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information" while not providing a definition of nonneural information and opening its potential coverage up to interpretation.

According to Montana SB 163 neurotechnology data is defined as that which "is captured by neurotechnologies, is generated by measuring the activity of an individual's central or peripheral nervous systems, or is data associated with neural activity, which means the activity of neurons or glial cells in the central or peripheral nervous system, and that is not nonneural information". Differently than the California amendment, Montana SB 163 also includes the definition for nonneural information[38] and facilitating interpretation regarding its possible coverage.

To illustrate, for example when electroencephalography (EEG) data is acquired from a consumer-grade device such as a headset for the purpose of inferring an individual's emotional state. Such data would be governed by the amended CCPA, however, the secondary processing of this inferred emotional state information might not be subject to the same statutory requirements.[39] This could be more clearly read from the Montana

[38] SB 163 defines nonneural information as "which means information about the downstream physical effects of neural activity, including by not limited to pupil dilation, motor activity, and breathing rate"
[39] Clark, Linda and Martinez, Carson, 'California Revises CCPA to Cover Neural Data' (*Morrison Foerster*, October 2024) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025.

amendment, under SB 163, considering an individual wearing an EEG headset during a memory test, the electrical signals generated by the brain in response to stimuli would be categorized as protected "neurotechnology data." However, a physiological manifestation like sweating would be classified as nonneural information and would not be covered by the amendments to Montana's Genetic Information Privacy Act (GIPA).[40]

B. Consent Requirements

By including neural data within sensitive data, the laws emphasize the need for explicit consent from individuals before collecting or using their neural data, particularly for non-medical contexts. Colorado and Montana's acts, for example, require initial express consent to collect or use neural data, and separate consent (or an opt-out option) before disclosing it to third parties.[41] This means a neurotech company should not just include brain data collection in the general terms of service, they must obtain clear permission, and sharing that data onward (i.e. to an analytics partner or data broker) requires additional user permission. Whereas the California's consent requirements under the CCPA treats sensitive data, therefore neural data, with a limited opt-out right however it covers it more broadly when it comes to employee's neural data, as it also falls under CCPA (unlike Colorado).[42]

[40] Clark, Linda, Crespo, Melissa and Wang, Katherine, 'Neural Data Added to Montana's Genetic Information Privacy Act' (*Morrison Foerster*, August 2025) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025.
[41] 'States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News' (n 21).
[42] 'Protecting the Mind - Exploring Brain Privacy Law' (*Morrison Foerster*, May 2024) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025.

C. Data Rights

The new statutes confer significant rights upon individuals, including the ability to access, delete, and withdraw consent for the processing of their neural data. Montana's legislation goes further by framing brain data as the property of the individual, thereby affirming ownership and control rights such as requiring a search warrant or subpoena based on probable cause for government access to neural data. Montana also differs in data localization and storage by prohibiting the storage of neural data in countries sanctioned by the US or designated as foreign adversaries.[43]

D. Restrictions on Use

The laws restrict certain applications of neural data that pose heightened ethical risks. For example, the Colorado amendment recognizes that neurotechnology raise privacy concerns "given their ability raise to monitor, decode, and manipulate brain activity". Whereas the California Assembly Committee's 2024 hearing looked into CCPA's application to neural data and included statements from The American Academy of Neurology, and the California Medical Association, referring to urgent need in protections for ethical handling of neural data.

[43] Clark, Linda, Crespo, Melissa and Wang, Katherine (n 40).

E. Transparency and Safeguards

Finally, the statutes mandate transparency and security. California integrated these protections into its California Consumer Privacy Act (as amended by the CPRA), while Colorado modified existing privacy laws to incorporate neural data and Montana amended the GIPA to include definitions of neural data. Notably, these reforms passed with overwhelming bipartisan support, reflecting a rare point of consensus in U.S. privacy lawmaking.[44] The acts call for companies to clearly disclose what neural data is collected, for what purposes, and must implement robust cybersecurity safeguards to protect against breaches and misuse.

F. Patchwork of Protections Pending Federal Effort

As early as 2005, a NYC Bar report looked into legal implications of neurotechnologies in the US and focused on "neuroprivacy".[45] By mid-2025, at least fifteen other states, including Alabama, Connecticut, Massachusetts, Minnesota, Illinois, and Vermont, were considering comparable legislation. Common themes include transparency requirements, explicit consent, individual rights of control, and prohibitions on exploitative uses of neural data. At the federal level, policymakers have held hearings,

[44] Cooley Law Firm, 'Wave of State Legislation Targets Mental Privacy and Neural Data' <https://www.cooley.com/news/insight/2025/2025-05-13-wave-of-state-legislation-targets-mental-privacy-and-neural-data> accessed 30 September 2025.
[45] 'Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging' (New York City Bar Committee on Science and Law 2005).

issued inquiries to regulators[46], and seen professional bodies such as the American Medical Association call for new safeguards.[47]

The result is an emerging patchwork regime: residents of states with neural privacy laws will soon enjoy strong protections, while those elsewhere remain vulnerable. This uneven landscape creates compliance challenges for neurotechnology companies and raises concerns about equality in the protection of cognitive privacy. While delayed, U.S. regulatory attention increasingly acknowledges that neural data represents a uniquely sensitive category requiring tailored legal safeguards.[48] The American Medical Association also adopted a policy in mid-2025 calling for greater regulation of neural data to protect patients and consumers. These developments suggest momentum toward possibly a federal neural data standard. Montana's law sponsor even described his bill as a "blueprint for a national neural data protection law".[49]

On the federal front, there is growing attention but not yet concrete action. In 2023 and 2024, U.S. Senators held hearings and sent inquiries to regulators about neurotechnology. A group of senators in 2025 urged the Federal Trade Commission (FTC) to investigate whether companies are improperly exploiting consumers' brain data.[50] In

[46] 'Sens. Cantwell, Schumer, Markey Introduce Legislation to Shield Americans' Brain Data From Exploitation' (*U.S. Senate Committee on Commerce, Science, & Transportation*, 24 September 2025) <https://www.commerce.senate.gov/2025/9/sens-cantwell-schumer-markey-introduce-legislation-to-shield-americans-brain-data-from-exploitation> accessed 1 October 2025.
[47] American Medical Association, 'Safeguarding Neural Data Collected by Neurotechnologies H-315.957' (2025) Resolution 503 A-25 <https://policysearch.ama-assn.org/policyfinder/detail/H-315.957?uri=%2FAMADoc%2FHOD.xml-H-315.957.xml>.
[48] Genser, Jared, Damianos, Stephen and Yuste, Rafael (n 5).
[49] 'States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News' (n 21).
[50] 'Sens. Cantwell, Schumer, Markey Introduce Legislation to Shield Americans' Brain Data From Exploitation' (n 46).

September 2025, the call to FTC was more formalized with the announced Management of Individual's Neural Data Act of 2025 (MIND Act).[51] [52] The proposed MIND Act aims to encourage responsible neurotechnology development and calls for "technical, procedural, and ethical safe-guards regarding each use case of such neurotechnology", as well as requiring guidance for "prohibited, permissible, and conditionally permitted use cases" of neurotechnology.

Section IV will examine how the European Union, which has a very different legal approach to the issue, is tackling the same challenge. However, first attention will be given to a case focusing on a U.S. company to illustrate privacy challenges of neurotech via a concrete example.

2. Case example: BrainCo, Student Attentiveness

To illustrate the U.S. regulatory status quo ante, consumer electroencephalography (EEG) headsets might provide a useful case study. These devices, marketed for applications ranging from meditation to gaming, are commonly integrated with companion applications and cloud-based analytics platforms. A 2024 report by the Neurorights Foundation examined the privacy policies of 30 such products and identified

[51] RIL25862 6FT. S.L.C.. 119TH CONGRESS. 1ST SESSION - A Bill to direct the Federal Trade Commission to conduct a study on the governance of neural data and other related data, and for other purposes 2025.
[52] Sara Pullen, 'Unlocking the MIND Act: The Senate To Take on the Challenge of Neurotechnology' (*Alston & Bird Privacy, Cyber & Data Strategy Blog*, 25 September 2025) <https://www.alstonprivacy.com/unlocking-the-mind-act-the-senate-to-take-on-the-challenge-of-neurotechnology/> accessed 1 October 2025.

widespread problematic practices.[53] The analysis revealed that 96.7% of companies claimed expansive rights of access to and use of users' neural data. The majority also expressly permitted data sharing with third parties, typically justified under vague formulations such as "for business purposes." Only two companies suggested any substantive limits to their access. Fewer than half of the firms afforded users a right to delete their data, and none provided clear explanations of why neural data constitutes a sensitive category or what forms of data were specifically collected. In practice, these companies relied on a notice-and-consent paradigm: once users accepted lengthy boilerplate terms, firms exercised virtually unrestricted discretion to monetize brain data.

A real-world incident further illustrates the risks posed by such regulatory lacunae. In 2019, media reports disclosed that BrainCo, a U.S.-based manufacturer of EEG headsets, had sold devices to schools in China, where students were instructed to wear headbands displaying colored lights indicating levels of attention. The episode provoked significant public backlash concerning student privacy and surveillance, ultimately leading the school to suspend the program. Although this incident occurred outside the United States, it resonated domestically as a cautionary example, particularly since no U.S. legal provisions at the time explicitly prohibited schools, or indeed employers, from deploying comparable practices. Only the subsequent wave of state-level neural data legislation has begun to render such uses unlawful, with several statutes explicitly banning compulsory neuro-monitoring in educational contexts.

[53] Genser, Jared, Damianos, Stephen and Yuste, Rafael (n 5).

This case exemplifies how social and ethical concerns can in some instances outpace legal protections. The imagery of children's brain activity being monitored in real time crystallized broader concerns and anxieties about cognitive privacy and surveillance, underscoring the urgency of regulatory intervention. Within the United States, this need is now being addressed primarily through fragmented state-level initiatives. Companies reviewed in the 2024 report will be compelled to revise their practices, such as limiting data sharing and honoring deletion requests, at least in jurisdictions with dedicated neural data laws. Whether industry stakeholders will ultimately advocate for a harmonized federal standard, thereby avoiding a patchwork of divergent state approaches, remains an open question.

IV. Legal Frameworks in the EU

Within the European Union (EU), privacy is not conceived merely as a consumer expectation but as a fundamental right enshrined in law. The central instrument governing data protection is the General Data Protection Regulation (GDPR)[54], in force since 2018, which establishes a uniform and comprehensive framework across all Member States and exerts considerable extraterritorial influence. The GDPR applies whenever "personal data", defined as information relating to an identified or identifiable natural person, is processed. Neural data collected through neurotechnological devices

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

will ordinarily meet this threshold, as such data are typically linked to an individual account or identity.

The GDPR imposes several core principles, including data minimization (limiting collection to what is strictly necessary), purpose limitation (restricting processing to specified purposes), and the requirement of a lawful basis for processing, such as informed consent or legitimate interest. Crucially, the GDPR recognizes certain categories of data as "special categories of personal data" that merit enhanced protection. These include health data and biometric data processed for identification purposes. Neural data, depending on its use and content, may fall within these categories. For example, electroencephalography (EEG) data collected in a clinical setting for diagnostic purposes clearly qualifies as health data under Article 4(15) GDPR, which defines such data as information "related to the physical or mental health of a natural person." By contrast, data derived from a consumer EEG headset used in gaming or wellness contexts presents greater ambiguity. EU regulators may initially treat it as ordinary personal data; however, if the data can be used to infer mental health conditions or impairments, it may acquire the status of health data.

A 2024 European Parliament study[55] emphasized that outside of the neurotechnology devices with a medical purpose that are covered under the Medical Device Regulation (MDR), when a demonstrable link to health exists, the data must be classified as health data under the GDPR, but in some cases absent such a link, the additional protections of

[55] European Parliament. Directorate General for Parliamentary Research Services. (n 1).

Article 9 GDPR may not apply. The study further suggested a possibility of considering "brain data" as an explicit new category of sensitive personal data if such a requirement results from in-depth investigation.

Despite these interpretive uncertainties, the GDPR already furnishes a stringent regulatory environment for neural data. Controllers processing such data within the EU must secure informed consent (or rely on another lawful ground), provide transparent information on data use, facilitate rights of access and erasure, implement appropriate security safeguards, and conduct data protection impact assessments where processing is high risk. Moreover, the principle of data protection by design and by default obliges neurotechnology developers to embed privacy-preserving features, such as on-device processing to minimize large-scale data transfers, into the technology itself. Enforcement is reinforced by the possibility of substantial administrative fines, up to 4% of global annual turnover, thereby incentivizing compliance among both established firms and emerging neurotechnology enterprises.

Nevertheless, the GDPR was drafted prior to the widespread emergence of consumer neurotechnology, and relies on its technology neutral broad coverage, but does not explicitly reference neural data. Scholars have argued that certain provisions may require refinement to adequately address the distinctive risks associated with neurodata.[56] For instance, the principle of purpose limitation may need to be interpreted more strictly in this context to prevent "function creep," whereby neural data collected for benign

[56] ibid.

purposes (e.g., wellness applications to improve focus by exercising with an EEG headband) could be repurposed for commercial profiling or advertising.[57] Similarly, the standard of informed consent may require elevation given the complexity and opacity of inferences that can be drawn from brain signals.

Beyond the data protection framework, the issue also engages the EU Charter of Fundamental Rights. Article 8 enshrines data protection, and Article 7 guarantees respect for private and family life, but some commentators contend that Article 10 (freedom of thought), mirroring Article 9 of the European Convention on Human Rights, may provide an additional, and potentially absolute, safeguard in the neurodigital era. Freedom of thought has traditionally been interpreted in relation to religion and belief, yet scholars increasingly argue that neurotechnologies capable of accessing or manipulating mental processes could also implicate this right.[58] Indeed, the EU has begun to explore this intersection; in 2023, EU institutions commissioned studies and hosted events addressing "freedom of thought in the neurodigital age." While case law is not yet developed, it is plausible that future litigation concerning neurotechnology will invoke not only data protection principles but also human dignity and freedom of thought.

In sum, the EU relies on a comprehensive rights-based framework rather than neuro-specific legislation. Although the GDPR does not explicitly enumerate "neural data," its broad definition of personal data and its recognition of special categories provide a

[57] The European Parliament study also emphasizes specific risks of using neural data repurposing regarding neurotechnology devices potential use in education with minors.
[58] Vera Tesink and others, 'Right to Mental Integrity and Neurotechnologies: Implications of the Extended Mind Thesis' (2024) 50 Journal of Medical Ethics 656.

strong baseline of protection. Consequently, companies operating in the EU face obligations, including erasure rights, data minimization, and restrictions on repurposing, that are significantly more stringent than those currently in place in the United States, save for certain state-level laws. This reflects Europe's proactive and rights-oriented approach: by embedding neurotechnology within the broader data protection regime, the EU has effectively created a legal architecture that safeguards neural data while leaving open the possibility of further refinement as technologies evolve.

1. Neuro-Specific Initiatives and Regulatory Efforts in Europe

Given General Data Protection Regulation (GDPR) providing a robust baseline, European policymakers have not approached neurotechnology with complacency. Instead, the European Union (EU) and its Member States have initiated neuro-specific measures, adapted existing legal frameworks, and engaged in broader rights-based debates to anticipate the distinctive risks posed by neurotechnologies.

A. Medical Device and Product Safety Regulations

The Medical Devices Regulation (MDR) 2017/745[59], which became fully applicable in 2021, explicitly extends its scope to certain neurotechnologies. In a notable regulatory

[59] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) 2025.

innovation, the MDR classifies even non-medical "brain stimulation" devices as high-risk medical devices (Class III). This means that transcranial electrical stimulators marketed for non-therapeutic purposes, such as enhancing concentration during gaming, must undergo rigorous clinical safety testing and obtain CE certification prior to market entry.[60]

The justification for this inclusion rests on the precautionary principle, recognizing that interventions which directly alter brain activity, regardless of whether they are therapeutic or recreational, pose inherent health and safety risks. While some industry stakeholders dispute the scientific basis for treating all neurostimulators as Class III devices, the MDR underscores the EU's willingness to preemptively regulate for safety and indirectly for privacy. Moreover, compliance under the MDR requires manufacturers to incorporate cybersecurity and data protection considerations. By contrast, "read-out" brain–computer interfaces (BCIs) that solely record neural activity without therapeutic purpose remain outside the MDR scope, instead falling under general consumer safety legislation and GDPR obligations.[61] Current discussions continue as to whether a dedicated legislative instrument for consumer neurodevices will eventually be necessary.

[60] Paheentharajah, Kokularajah and Martens, Julia (n 14).
[61] ibid.

B. The AI Act and Subliminal Manipulation

The EU Artificial Intelligence Act (AI Act)[62], represents a second pillar of EU neurotech governance. The Act prohibits AI systems that employ subliminal techniques in ways that materially distort human behavior and cause harm, as well as systems that exploit the vulnerabilities of specific groups. These provisions plausibly encompass neurotechnologies integrated with AI, particularly those designed to manipulate cognition or decision-making.

For example, AI-driven neurofeedback systems that subtly nudge user choices through subliminal stimuli, already explored in neuromarketing research, would fall within this prohibition. The AI Act also classifies certain applications as "high-risk," including biometric identification and systems used in employment or education. Importantly, it bans AI-based emotion recognition in policing, employment, and educational contexts, save for limited exceptions. This is highly relevant given that many neurotechnologies advertise emotion-recognition capabilities, such as EEG devices purporting to assess worker engagement or such as BrainCo, as discussed in Section III.2. deployed in education. A recent report[63] also highlighted that a potential risk of EEG use might also include its prospective for predicting voting behavior.[64] Given these sensitive use cases,

[62] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) 2024.
[63] Antonia Mochan and others, 'Emerging Applications of Neurotechnology and Their Implications for EU Governance' (*JRC Publications Repository*, 2025) <https://publications.jrc.ec.europa.eu/repository/handle/JRC141928> accessed 2 October 2025.
[64] Giulia Galli and others, 'Early EEG Responses to Pre-Electoral Survey Items Reflect Political Attitudes and Predict Voting Behavior' (2021) 11 Scientific Reports 18692.

the AI Act indirectly strengthens mental privacy protections by restricting manipulative and high-risk applications, complementing the GDPR's focus on data handling.

C. Human Rights Discourse and Neurorights

Europe has also been a central forum for neuroethics and neurorights debates. The Council of Europe's Bioethics Committee examined neurotechnologies between 2019 and 2022, producing a report that considered whether additional protocols or recommendations might be necessary under the European Convention on Human Rights to safeguard cognitive liberty and mental privacy. Although no binding instrument has yet resulted, this reflects Europe's leadership in framing neurotechnology as a human rights issue.

At the EU level, the European Parliament has commissioned studies and debated neurorights, while several Member States have adopted non-binding charters. Spain's 2021 Digital Rights Charter[65] explicitly acknowledged neurorights, including mental privacy, self-determination and the protection of neural data, as guiding principles. France followed in 2022 with a Charter for the Responsible Development of Neurotechnologies[66], outlining ethical commitments around consent, equity, and fairness as well as protections against potentially abusive and malicious use of neural

[65] 'Charter of Digital Rights' (Government of Spain 2021) <https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/SPAIN_Charter-of-Digital-Rights.pdf>.

[66] 'Présentation de la charte française de l'innovation responsable en neurotechnologies' (*enseignementsup-recherche.gouv.fr*) <https://www.enseignementsup-recherche.gouv.fr/fr/presentation-de-la-charte-francaise-de-l-innovation-responsable-en-neurotechnologies-87967> accessed 2 October 2025.

data. In 2023, the León Declaration, endorsed by the Council of the European Union[67], reaffirmed a "human-centric" approach to neurotechnology and a commitment to protecting fundamental rights. Although these texts lack legal force, they illustrate strong political will and may inform future regulatory developments.

2. The Absence of a Dedicated EU Neurotechnology Law

Despite these initiatives, the EU has not enacted a standalone Neurotechnology Act or amended GDPR specifically to address neural data. The prevailing view among policymakers has been that existing frameworks, GDPR, human rights law, MDR, and the AI Act, already provide sufficient legal instruments. Many European jurists caution against fragmenting fundamental rights into narrowly defined "neurorights," warning that such an approach may inadvertently weaken established protections or create interpretive gaps. Instead, the dominant strategy has been to interpret existing rights, such as privacy (Article 8 ECHR) and freedom of thought (Article 9 ECHR), in light of neurotechnological challenges.

Nevertheless, advocacy groups and some scholars argue for explicit legal recognition of neurorights to ensure comprehensive coverage and avoid ambiguity.[68] The debate thus reflects a tension between a principles-based approach, relying on established rights

[67] 'TechDispatch #1/2024 - Neurodata | European Data Protection Supervisor' (1 October 2025) <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata> accessed 2 October 2025.
[68] Ligthart and others (n 3).

and flexible interpretation, and a codification approach, favoring explicit enumeration of novel rights.

Taken together, Europe's response can be described as precautionary and principles-driven. The EU has demonstrated willingness to impose strict ex ante requirements, such as the MDR's high-risk classification for brain stimulation devices and the AI Act's categorical bans on manipulative systems. At the same time, regulators emphasize reliance on broad, rights-based frameworks rather than piecemeal legislation for each technological development. The guiding question remains whether neurotechnologies pose risks to autonomy, dignity, or privacy, and if so, how existing rights can be interpreted to address them.

Europe's trajectory is also shaped by developments abroad. Notably, Chile became the first country in 2021 to enshrine neurorights in its constitution, explicitly protecting mental integrity and the privacy of brain data. This precedent, alongside the advocacy of initiatives such as the NeuroRights Foundation, has informed European debates and inspired domestic initiatives in Spain and France. International organizations are likewise engaging: UNESCO is developing a global ethical framework, the OECD issued neurotechnology principles in 2019, and in 2025 the UN Special Rapporteur on Privacy urged states to adopt dedicated neurotechnology rules. The UN Human Rights Council's Advisory Committee has also recommended developing authoritative interpretations of freedom of thought in the neurotechnological context.

Given Europe's strong tradition of aligning domestic law with international human rights standards, it is likely that these global initiatives will further influence the EU's regulatory evolution. While a dedicated EU neurotechnology statute has not yet emerged, ongoing discourse suggests that refinement, whether through guidelines, interpretive standards, or new legislation, remains a distinct possibility.

3. Case Example: EU Workplace monitoring Devices

An article referring to French data protection authority's (CNIL) stance on neurowearables at work, essentially warning employers that measuring brain activity of employees could violate human dignity and privacy as per the French Labour Code and Data Protection Act given the principle of proportionality[69], and that less intrusive means should be used to ensure well-being and safety (this was in response to some proposals to use fatigue-monitoring headbands for truck drivers, for example). Under the AI Act, if the device's AI tried to infer emotions or attention for evaluation of workers, that would be outright banned. Thus, our hypothetical company, to comply in the EU, might drastically alter the program: making it strictly opt-in with no consequences for non-use, anonymizing and aggregating the data so no individual profiles are created, and using it only for personal feedback to the employee rather than for management oversight. Even then, it would be treading carefully, and perhaps it would abandon the idea altogether as more trouble than it's worth. This contrast shows how the EU's robust legal framework

[69] 'Quelles Limites Pour La Surveillance Connectée Au Travail ? | Linc' <https://linc.cnil.fr/quelles-limites-pour-la-surveillance-connectee-au-travail> accessed 2 October 2025.

can serve as a deterrent against potential neurotech-enabled privacy invasions in sensitive contexts[70] (like employment), whereas in the U.S., until recently, there was little beyond public backlash to act as a check. With new state laws (e.g. some explicitly banning workplace neural monitoring without consent or even entirely), the U.S. is starting to move closer to the EU stance on this specific issue.

V. Towards a Transatlantic Regulatory Framework

1. Ethical and Societal Implications

A. Ethical Issues

Regarding the privacy implications of neurotechnology, both the United States and the European Union recognize a shared set of ethical concerns, though these are often framed differently according to their respective legal traditions, cultural contexts, and philosophical orientations. This section explores the central ethical principles, often described under the umbrella of "neurorights"[71], as well as the broader societal issues raised by neurotechnological innovation.[72]

[70] Sjors Ligthart, 'Freedom of Thought in Europe: Do Advances in "Brain-Reading" Technology Call for Revision?' (2020) 7 Journal of Law and the Biosciences lsaa048.
[71] Genser, Jared, Damianos, Stephen and Yuste, Rafael (n 5).
[72] Ligthart and others (n 3).

B. Ethical Principles and Neurorights

Over the past two decades, neuroethics has crystallized into a distinct field, anticipating many of the dilemmas now at the forefront of policy debates. A seminal contribution to this discourse is the articulation of four potential neurorights[73]: cognitive liberty, mental privacy, mental integrity, and psychological continuity. While these concepts align with existing human rights, they highlight the specific vulnerabilities posed by neural data and brain–computer interaction.

i. Cognitive Liberty

Cognitive liberty refers to the freedom of individuals to control their own mental processes and to choose whether, and how, to employ neurotechnological tools.[74] It encompasses both the right to enhance cognition voluntarily and the right to be free from coercive interference. In the U.S., this concept is often tied to values of self-determination and sometimes linked to First Amendment protections of freedom of thought. In the EU, cognitive liberty resonates with the rights to autonomy and human dignity enshrined in fundamental rights law.

[73] Ienca and Andorno (n 15).
[74] Ligthart and others (n 3).

ii. Mental Privacy

Mental privacy denotes the right to keep one's neural activity and inner thoughts free from intrusion, disclosure, or appropriation.[75] It requires protection from both unauthorized access to neural data and its exploitation for external purposes. The ethical consensus is that mental privacy is foundational for autonomy and free will. International bodies such as UNESCO and the UN Special Rapporteur on Privacy have called for explicit recognition of this principle. In Europe, it is typically framed within the broader rights to privacy and freedom of thought; in the U.S., it is often discussed as an extension of cognitive liberty or mental health rights.

iii. Mental Integrity

Mental integrity refers to protection against unauthorized manipulation or harm to one's mental processes. Analogous to bodily integrity, it guards against technologies that could alter neural states without consent, such as hacked brain implants or subliminal neurostimulation. European documents often emphasize mental integrity alongside dignity, and Spain's Digital Rights Charter specifically highlights the need to safeguard citizens against neurotechnologies that could compromise their mental integrity.

[75] ibid.

vi. Psychological Continuity

Psychological continuity is the right to preserve one's sense of identity and coherence of self over time.[76] This principle addresses concerns that neurotechnologies could disrupt personal identity through unintended personality changes, dependency, or identity confusion. Although less frequently referenced in formal policy, it remains central to ethical debates regarding long-term personhood and the implications of cognitive enhancement.

Across both the U.S. and EU, scholars and policymakers have invoked these neurorights in different ways. U.S. advocates, such as Nita Farahany, have explicitly argued for the legal recognition of cognitive liberty[77], while European scholars, including Marcello Ienca and Roberto Andorno, who coined the four neurorights framework[78], have shaped debates within the Council of Europe. The transatlantic convergence on the importance of these principles is evident in certain governance initiatives discussed in this article, even as the mechanisms for legal implementation diverge.

A central debate concerns whether neurorights should be codified as distinct legal entitlements or interpreted through existing rights frameworks. European institutions tend to prefer reinterpretation, warning against proliferating new rights categories that may fragment protections. In contrast, certain advocates in the U.S. are more inclined to

[76] Ienca and Andorno (n 15).
[77] Farahany (n 13).
[78] Ienca and Andorno (n 15).

propose neurorights as novel legal constructs, reflecting the absence of constitutional recognition of privacy as a fundamental right.

C. Societal Implications

Beyond individual rights, neurotechnology raises broader societal questions relating to surveillance, trust, healthcare, cultural values, and governance structures.

i. Surveillance and Control

One of the most significant fears is the potential for neurotechnology to be employed as a tool of surveillance or coercive social control. Pilot programs in China involving EEG monitoring of students and workers have heightened global anxieties.[79] In response, European regulators have preemptively banned emotion-recognition AI in sensitive contexts, while in the U.S., the Fourth Amendment may constrain state use of neural data but provides little protection in the private sector absent specific legislation. Social resistance to "mind surveillance" is strong on both continents, though Europe has embedded legal safeguards earlier and more explicitly.

[79] Genser, Jared, Damianos, Stephen and Yuste, Rafael (n 5).

ii. Public Trust in Technology

Societal acceptance of neurotechnology depends heavily on trust. Privacy scandals, whether in the social media sector or future neurotech contexts, have the potential to erode public confidence. European consumers, traditionally more privacy-conscious, may be reluctant to adopt neurotechnologies without strong legal assurances, whereas Americans may initially embrace such technologies but react strongly to perceived misuse, as seen with the fallout from Cambridge Analytica. Policymakers on both sides emphasize balancing innovation with rights protection, recognizing that trust is essential for uptake.

iii. Healthcare and Equity

Neurotechnologies hold promise in clinical contexts, but their integration into consumer markets raises equity and privacy challenges.[80] The EU's regulatory frameworks classify much neural data as health data, while the U.S. relies on HIPAA only in medical settings. This leaves gaps when consumer neurotech data may later be repurposed for health-related uses, such as by insurers. Beyond privacy, access and affordability raise ethical concerns. Without deliberate policies, neurotechnologies risk exacerbating social inequalities, an issue UNESCO has explicitly warned against.

[80] Anita S Jwa and Nicole Martinez-Martin, 'Rationales and Approaches to Protecting Brain Data: A Scoping Review' (2023) 17 Neuroethics 2.

iv. Cultural Conceptions of Privacy

Cultural traditions shape how societies frame neuroprivacy. In Europe, thought privacy is linked to dignity and the inviolability of conscience, informed by historical experiences with totalitarian regimes. In the U.S., it is framed more in terms of liberty and resistance to government overreach. Despite these differences, both societies share a deep-seated conviction that mental privacy must remain sacrosanct.

v. Democratization versus Commercialization

Finally, societal debates address who controls neurotechnology and its data. Should ownership reside with individuals, corporations, or states? The EU model emphasizes strong user rights under GDPR, while several U.S. states have gone further, framing brain data explicitly as the property of the individual. This contest between democratization and commercialization will shape adoption: individuals are unlikely to embrace neurotechnology if they perceive it as primarily serving corporate or governmental interests.

Across both the United States and the European Union, there is growing consensus that neurotechnology requires ethical frameworks and societal safeguards extending beyond legal compliance. While the EU pursues a precautionary, rights-based approach and the U.S. remains more pluralist and innovation-driven, both systems are converging on the view that mental privacy, cognitive liberty, and human dignity represent non-negotiable principles. The key challenge is operationalizing these ideals into enforceable protections that can guide innovation without undermining fundamental rights.

D. International Landscape

Governance of the risks neural data proposes received international attention in the recent years from many organizations such as the OECD, UNESCO, and International Working Group on Data Protection in Technology.[81] Worldwide attention to the subject was also translated in codified law, for example in Chile in 2021, making it the first country adopting an amendment to its constitution for neural data.[82]

The UNESCO guidelines[83] define neural data as "qualitative and quantitative data about the structure, activity and function of the nervous system gathered through neurotechnology..." and highlights that "nonneural data allowing cognitive states inferences" raise similar ethical and human rights issues to neurotechnology. The guidelines call for the member states to "proactively establish a regulatory framework that balances innovation in the recreational and commercial domains with protecting individual rights and well-being".

In 2025, OECD published its Neurotechnology Toolkit[84] building on its former recommendations[85] on responsible innovation in neurotechnology. The 2019 recommendations made a call for prioritizing safety assessment, safeguarding personal

[81] 'Neurotechnologies, Du Champ Des Possibles Aux Projets de Régulation | Linc' <https://linc.cnil.fr/neurotechnologies-du-champ-des-possibles-aux-projets-de-regulation> accessed 2 October 2025.
[82] 'States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News' (n 21).
[83] UNESCO (n 10).
[84] 'Neurotechnology Toolkit' (OECD 2025) <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf>.
[85] 'Recommendation of the Council on Responsible Innovation in Neurotechnology' (OECD 2019) OECD/LEGAL/0457 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457>.

brain data and anticipating as well as monitoring potential malicious uses. In these recommendations personal brain data was defined as "data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states". The 2025 Toolkit focuses on actionable guidelines on addressing these issues and includes suggestions such as implementing a "safety by design" approach to both neurotechnology development and post-market oversight (i.e. through red teaming exercises).

An extensive working paper from the International Working Group on Data Protection in Technology recognizes global calls for "neurorights".[86] The working paper also emphasizes newer and lesser discussed important risks such as "neurodiscrimination" and defines it as a result of systemic bias that could arise from the use of algorithms to analyse neurodata. In addition to advocating for "fair access to neuroaugmentation", which would refer to mental augmentation for example that would ease symptoms of neurodegenerative diseases or even help with treating depression.[87]

It is important to note that while the international governance efforts are highly valuable for charting the way forward, they are not enforceable. Whereas the constitutional amendment in Chile, not only codified the definition and protection of neural data in

[86] 'Working Paper on Emerging Neurotechnologies and Data Protection' (IWGDPT 2025) <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20250515-WP-Neurotechnologies.pd>.
[87] Oliva Scott, 'Understanding the Debate on Fair Access to Mental Augmentation in Neurotechnology - Alliance for Citizen Engagement' (13 November 2024) <https://ace-usa.org/blog/research/research-technology/understanding-the-debate-on-fair-access-to-mental-augmentation-in-neurotechnology/, https://ace-usa.org/blog/research/research-technology/understanding-the-debate-on-fair-access-to-mental-augmentation-in-neurotechnology/> accessed 2 October 2025.

2021[88], but also already led to an enforcement example by its Supreme Court in 2023.[89] Chilean Senator Guido Girardi proposed a constitutional provision which was then enshrined in the Chile constitution as a protection for brain activity. In 2023, the Chilean Supreme Court ordered a US producer of a brain scanning tool, Emotiv, to erase the data it had collected on Guido Girardi.[90]

E. The way-forward

The governance of neurotechnology is increasingly framed not only as a domestic regulatory question but also as part of transatlantic cooperation. Since its launch in 2021, the EU–U.S. Trade and Technology Council (TTC)[91] was functioning as the primary forum for aligning approaches to emerging technologies, including artificial intelligence, data governance, and digital rights. While neurotechnology was not a headline item, the TTC's emphasis on "trustworthy technology" and "human-centric innovation" might provide a natural foundation for incorporating neural data and cognitive privacy into its agenda. Former TTC dialogues already touched upon adjacent domains such as AI risk management, cybersecurity, and biotechnology regulation, all of which intersect with neurotechnology. Given the TTC's role as a venue for harmonization and standard-setting, the comparative trajectories of the U.S. and EU on neuroprivacy are not merely

[88] Ligthart and others (n 3).
[89] 'Hands off My Brainwaves: Latin America in Race for "neurorights" | Reuters' <https://www.reuters.com/article/technology/hands-off-my-brainwaves-latin-america-in-race-for-neurorights-idUSL8N3AH6D6/> accessed 2 October 2025.
[90] ibid.
[91] EU-US TTC, 'TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management' (2022).

parallel but potentially convergent, with transatlantic collaboration potentially serving as a catalyst and possibly informing global norms.

Having examined each jurisdiction in detail, this section contrasts the United States and the European Union across regulatory philosophy, legal coverage, enforcement architectures, underlying conceptual frameworks, technological scope, public engagement, and industry responses, and concludes with observations about prospective convergence.

i. Regulatory Approaches

The EU proceeds from a comprehensive, fundamental-rights orientation in which privacy is constitutionally grounded and technologies that implicate it are assessed within that framework. This yields broad, horizontally applicable instruments (e.g., GDPR, the AI Act) and a willingness to regulate proactively where risks are credible, illustrated by bringing certain BCIs within the MDR and banning manipulative AI practices . By contrast, the U.S. tradition is sectoral and reactive, historically favoring innovation and intervening post hoc when harms materialize. Recent state-level neural privacy statutes, however, reflect a notable departure: bipartisan coalitions have acted pre-emptively in view of the exceptional sensitivity of cognitive data. Absent a federal statute, the U.S. landscape remains fragmented.

ii. Scope and Enforcement

At present, EU residents enjoy comparatively uniform and robust protection for neural data. GDPR and human-rights norms apply across Member States, affording clear rights and remedies to a Spanish or German user whose brain data are misused. In the U.S., coverage varies by state: Californians and Coloradans may be securing protections comparable to Europe, while residents elsewhere may not. Federal proposals have not yet been enacted; consequently, the EU baseline is high and consistent, whereas the U.S. is moving from low to medium protection in a piecemeal fashion.

EU enforcement is institutionalized: national Data Protection Authorities investigate, order remedial measures, and levy significant administrative fines under GDPR. Individuals can complain to DPAs and seek judicial redress. In the U.S., the Federal Trade Commission traditionally polices unfair or deceptive practices, a comparatively blunt tool for novel contexts, and typically operates ex post. New state neural privacy laws empower state Attorneys General and, in some instances, authorize private litigation (mirroring the deterrent effect seen under Illinois's BIPA). Class actions remain a distinctive U.S. mechanism, while collective redress in the EU is developing but less mature. Overall, both systems are trending toward more vigorous enforcement, though EU regulators possess a clearer mandate to treat neural data breaches as serious infractions.

F. Choices Ahead: New Rights vs. Extension of Existing Rights

The EU generally resists proliferating novel rights categories, instead interpreting existing guarantees, privacy, dignity, and freedom of thought, as encompassing neuro-specific concerns. U.S. discourse is more open to articulating neurorights as freestanding statutory entitlements (e.g., an explicit right to mental privacy or freedom from AI-induced manipulation). The divergence reflects legal culture more than substance: Europe is likely to continue refining and enforcing its composite framework; the U.S. may ultimately adopt an expressly titled federal "neural rights" or "neural data" statute.

i. Security Oversight

Both jurisdictions address invasive and non-invasive systems, but the EU has explicitly brought certain non-medical neurostimulation devices into the MDR as Class III high-risk products. The U.S. Food and Drug Administration typically refrains from regulating wellness devices lacking medical claims, leaving a safety and (indirect) privacy gap for some consumer neurostimulators and neurofeedback tools. State neural data laws focus on information governance rather than device safety. Accordingly, EU users may be better insulated from unsafe or unproven devices, while U.S. consumers encounter a more permissive market, though FDA jurisdiction expands when diagnostic or therapeutic claims arise.

ii. Industry Focus

EU-based firms design their products in light of GDPR and (prospectively) AI Act constraints, sometimes touting privacy-by-design as a competitive differentiator and orienting toward medical pathways with clearer regulatory routes. Consumer neurotech offerings face higher compliance costs (e.g., MDR), which may deter marginal entrants. U.S. firms historically iterated more freely, accelerating consumer-facing experimentation; with state laws, however, they must now embed granular consent, minimize sharing, and/or geofence functionality. Prominent actors have adjusted trajectories (e.g., pivoting away from direct brain-signal capture) in recognition of reputational and legal risks. Across both markets, public acceptance might increasingly hinge on demonstrable privacy assurances.

The EU's rights-based, precautionary architecture (GDPR, AI Act, MDR, and fundamental rights enshrined in EU Charters) delivers a holistic governance envelope for neurotechnology, covering data protection, manipulative uses, and device safety, while the U.S. is assembling a functionally similar mosaic through state privacy statutes, sectoral oversight (FDA), professional ethics, and potential federal action. Multilateral fora (OECD, UNESCO) and comparative exemplars (e.g., Chile's constitutional neurorights) are catalyzing alignment on definitions, consent norms, prohibited practices, and equity considerations. Given that public trust is a prerequisite for adoption, both jurisdictions are converging on the imperative to foreground mental privacy and human dignity as organizing principles for neurotechnology governance.

VI. Conclusion

Neurotechnology is frequently characterized as the “next frontier” of human innovation, offering unprecedented opportunities to restore function, enhance cognition, and transform aspects of daily life. Yet, as this analysis has demonstrated, it simultaneously represents a frontier of privacy. Both the United States and the European Union, despite their divergent legal traditions, exhibit a shared recognition of the need to safeguard the inner domain of thought against the risks posed by emerging neurotechnologies. The U.S. trajectory reflects a gradual transition from sector-specific and fragmented protections toward more unified approaches at the state level, with prospects for eventual federal harmonization. The EU, by contrast, relies on its comprehensive data protection framework and deeply embedded human rights commitments to extend existing principles to the governance of neural data. Across both jurisdictions, the core challenge lies in reconciling technological innovation with the imperatives of autonomy, dignity, and mental integrity.

Several themes emerge from this comparative inquiry. First, mental privacy and cognitive liberty are increasingly articulated not merely as philosophical constructs but as actionable legal rights. Montana’s statutory declaration of individual ownership of brain data [64] and the EU’s prohibition on subliminal AI manipulation [98] exemplify this trend. Second, legal adaptability is evident on both sides of the Atlantic: established principles, ranging from the privilege against self-incrimination to the GDPR’s principle of data minimization, are being reinterpreted in light of neurotechnological developments. Third,

investigations into consumer neurotechnology firms' inadequate data practices [55], as well as high-profile uses of devices in classrooms and workplaces, have served as cautionary episodes accelerating regulatory responses.

Policymakers in both sides of the Atlantic affirm the exceptional status of the brain as a locus of personhood and autonomy, warranting enhanced protection. This shared normative stance suggests the possibility of establishing a transatlantic baseline of mental privacy and cognitive liberty as guiding principles for neurotechnology's societal integration. Nevertheless, challenges persist: effective enforcement must accompany new rules; legal frameworks must adapt to address evolving use cases (including cross-border data flows and unforeseen applications); and public education, alongside industry compliance, will be critical to fostering responsible adoption. International coordination will also be indispensable, given that neural data, like other forms of digital information, transcends jurisdictional boundaries.

The comparative analysis indicates that while neither system is flawless, both offer valuable insights. The United States demonstrates the utility of federalism and policy experimentation, with state-level statutes introducing innovative consent requirements and workplace protections that may inform future European guidance. The EU, by contrast, exemplifies the advantages of a comprehensive, rights-based regime, offering clarity and consistency that could inspire U.S. efforts toward a federal standard to avoid regulatory fragmentation. Both approaches underscore the capacity of democratic societies to act preemptively to mitigate emergent risks, rather than deferring intervention until harms are entrenched.

Looking ahead, as neurotechnology advances, from restoring speech in locked-in patients to the speculative prospect of direct neural control of consumer devices, the primacy of privacy will remain paramount. This study highlights the importance of continuous interdisciplinary research, inclusive public dialogue, and sustained international cooperation to ensure that governance keeps pace with innovation. The ultimate objective, common to both the U.S. and EU, is to realize the profound benefits of neurotechnology while safeguarding the fundamental right to mental privacy. In this sense, the comparative analysis reveals more convergence than divergence: the legal instruments and regulatory timetables may differ, but both systems are moving decisively toward stronger protection of the self in the neurotechnological era. By learning from one another and drawing on empirical experiences, the transatlantic partners are well positioned to lead the development of governance models that preserve human dignity in an age of rapid neuroscientific progress.

Finally, the EU–U.S. Trade and Technology Council (TTC) or a similar framework might offer a promising institutional platform through which this convergence could be operationalized. While neurotechnology has not yet featured prominently on the TTC agenda, its previous work on artificial intelligence, data governance, and trustworthy technology provides a natural entry point. Incorporating neurotechnology into transatlantic dialogues would allow the U.S. and EU to harmonize definitions, align safeguards, and jointly articulate standards for mental privacy and cognitive liberty. In doing so, the transatlantic partners could extend their leadership beyond their domestic

frameworks to set global norms, ensuring that the benefits of neurotechnology are realized without compromising the integrity of the human mind.

References

American Medical Association, ‘Safeguarding Neural Data Collected by Neurotechnologies H-315.957’ (2025) Resolution 503 A-25 <https://policysearch.ama-assn.org/policyfinder/detail/H-315.957?uri=%2FAMADoc%2FHOD.xml-H-315.957.xml>

‘Are Your Thoughts Your Own?: “Neuroprivacy” and the Legal Implications of Brain Imaging’ (New York City Bar Committee on Science and Law 2005)

Birbaumer N, ‘Breaking the Silence: Brain-Computer Interfaces (BCI) for Communication and Motor Control’ (2006) 43 Psychophysiology 517

‘Charter of Digital Rights’ (Government of Spain 2021) <https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/SPAIN_Charter-of-Digital-Rights.pdf>

Clark, Linda, Crespo, Melissa and Wang, Katherine, ‘Neural Data Added to Montana’s Genetic Information Privacy Act’ (*Morrison Foerster*, August 2025) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025

Clark, Linda and Martinez, Carson, ‘California Revises CCPA to Cover Neural Data’ (*Morrison Foerster*, October 2024) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025

Cooley Law Firm, ‘Wave of State Legislation Targets Mental Privacy and Neural Data’ <https://www.cooley.com/news/insight/2025/2025-05-13-wave-of-state-legislation-targets-mental-privacy-and-neural-data> accessed 30 September 2025

‘Ethics of Neurotechnology | UNESCO’ <https://www.unesco.org/en/ethics-neurotech> accessed 30 September 2025

European Parliament. Directorate General for Parliamentary Research Services., *The Protection of Mental Privacy in the Area of Neuroscience: Societal, Legal and Ethical Challenges.* (Publications Office 2024) <https://data.europa.eu/doi/10.2861/869928> accessed 30 September 2025

Farahany N, ‘The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology’ [2023] Faculty Books

Farahany NA, ‘Incriminating Thoughts’ (2012) 64 Stanford Law Review 351

Galli G and others, ‘Early EEG Responses to Pre-Electoral Survey Items Reflect Political Attitudes and Predict Voting Behavior’ (2021) 11 Scientific Reports 18692

Genser, Jared, Damianos, Stephen and Yuste, Rafael, ‘Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies’ (Neurorights Foundation 2024)

‘Hands off My Brainwaves: Latin America in Race for “neurorights” | Reuters’ <https://www.reuters.com/article/technology/hands-off-my-brainwaves-latin-america-in-race-for-neurorights-idUSL8N3AH6D6/> accessed 2 October 2025

Ienca M and Andorno R, ‘Towards New Human Rights in the Age of Neuroscience and Neurotechnology’ (2017) 13 Life Sciences, Society and Policy 5

Ienca M and Haselager P, ‘Hacking the Brain: Brain–Computer Interfacing Technology and the Ethics of Neurosecurity’ (2016) 18 Ethics and Information Technology 117

Istace T, ‘Protecting the Mental Realm: What Does Human Rights Law Bring to the Table?’ (2023) 41 Netherlands Quarterly of Human Rights 214

Jwa AS and Martinez-Martin N, ‘Rationales and Approaches to Protecting Brain Data: A Scoping Review’ (2023) 17 Neuroethics 2

Ligthart S, ‘Freedom of Thought in Europe: Do Advances in “Brain-Reading” Technology Call for Revision?’ (2020) 7 Journal of Law and the Biosciences lsaa048

——, ‘Minding Rights: Mapping Ethical and Legal Foundations of “Neurorights”’ (2023) 32 Cambridge Quarterly of Healthcare Ethics 461

Mochan A and others, ‘Emerging Applications of Neurotechnology and Their Implications for EU Governance’ (*JRC Publications Repository*, 2025) <https://publications.jrc.ec.europa.eu/repository/handle/JRC141928> accessed 2 October 2025

Murphy ERD and Rissman J, ‘Evidence of Memory from Brain Data’ (2020) 7 Journal of Law and the Biosciences lsaa078

‘Neurotechnologies, Du Champ Des Possibles Aux Projets de Régulation | Linc’ <https://linc.cnil.fr/neurotechnologies-du-champ-des-possibles-aux-projets-de-regulation> accessed 2 October 2025

‘Neurotechnology Toolkit’ (OECD 2025) <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf>

Paheenthararajah, Kokularajah and Martens, Julia, ‘Ethical and Legal Challenges of Neurotech’ (*DLA Piper*, 27 March 2025) <https://www.dlapiper.com/en/insights/publications/2025/03/ethical-and-legal-challenges-of-neurotech> accessed 30 September 2025

Patrick-Krueger KM, Burkhart I and Contreras-Vidal JL, ‘The State of Clinical Trials of Implantable Brain–Computer Interfaces’ (2025) 3 Nature Reviews Bioengineering 50

‘Présentation de la charte française de l’innovation responsable en neurotechnologies’ (*enseignementsup-recherche.gouv.fr*) <https://www.enseignementsup-recherche.gouv.fr/fr/presentation-de-la-charte-francaise-de-l-innovation-responsable-en-neurotechnologies-87967> accessed 2 October 2025

‘Protecting the Mind - Exploring Brain Privacy Law’ (*Morrison Foerster*, May 2024) <https://www.mofo.com/resources/insights/null> accessed 1 October 2025

Pullen S, ‘Unlocking the MIND Act: The Senate To Take on the Challenge of Neurotechnology’ (*Alston & Bird Privacy, Cyber & Data Strategy Blog*, 25 September 2025) <https://www.alstonprivacy.com/unlocking-the-mind-act-the-senate-to-take-on-the-challenge-of-neurotechnology/> accessed 1 October 2025

‘Quelles Limites Pour La Surveillance Connectée Au Travail ? | Linc’ <https://linc.cnil.fr/quelles-limites-pour-la-surveillance-connectee-au-travail> accessed 2 October 2025

‘Recommendation of the Council on Responsible Innovation in Neurotechnology’ (OECD 2019) OECD/LEGAL/0457 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457>

Ruiz S and others, ‘Neurorights in the Constitution: From Neurotechnology to Ethics and Politics’ (2024) 379 Philosophical Transactions of the Royal Society B: Biological Sciences 20230098

Scott O, ‘Understanding the Debate on Fair Access to Mental Augmentation in Neurotechnology - Alliance for Citizen Engagement’ (13 November 2024) <https://ace-usa.org/blog/research/research-technology/understanding-the-debate-on-fair-access-to-mental-augmentation-in-neurotechnology/, https://ace-usa.org/blog/research/research-technology/understanding-the-debate-on-fair-access-to-mental-augmentation-in-neurotechnology/> accessed 2 October 2025

‘Sens. Cantwell, Schumer, Markey Introduce Legislation to Shield Americans’ Brain Data From Exploitation’ (*U.S. Senate Committee on Commerce, Science, & Transportation*, 24 September 2025) <https://www.commerce.senate.gov/2025/9/sens-cantwell-schumer-markey-introduce-legislation-to-shield-americans-brain-data-from-exploitation> accessed 1 October 2025

‘States Pass Privacy Laws to Protect Brain Data Collected by Devices - CBS News’ (16 July 2025) <https://www.cbsnews.com/news/state-privacy-laws-brain-data-devices/> accessed 30 September 2025

Szoszkiewicz Ł and Yuste R, ‘Mental Privacy: Navigating Risks, Rights and Regulation’ (2025) 26 EMBO Reports 3469

‘TechDispatch #1/2024 - Neurodata | European Data Protection Supervisor’ (1 October 2025) <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata> accessed 2 October 2025

Tesink V and others, ‘Right to Mental Integrity and Neurotechnologies: Implications of the Extended Mind Thesis’ (2024) 50 Journal of Medical Ethics 656

UNESCO, ‘Draft Recommendation on the Ethics of Neurotechnology - UNESCO Digital Library’ (2025) <https://unesdoc.unesco.org/ark:/48223/pf0000394866> accessed 30 September 2025

‘Working Paper on Emerging Neurotechnologies and Data Protection’ (IWGDPT 2025) <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20250515-WP-Neurotechnologies.pd>

California SB 1223 An act to amend Section 1798.140 of the Civil Code, relating to privacy [SB 1223]

Colorado House Bill 24-1058 An act concerning protecting the privacy of individuals' biological data, and, in connection therewith, protecting the privacy of neural data and expanding the scope of the 'Colorado Privacy Act' accordingly [HB24-1058]

Montana SB 163 An act revising the genetic information privacy act; including neurotechnology data in the scope of the genetic information privacy act [SB163]

RIL25862 6FT. S.L.C.. 119TH CONGRESS. 1ST SESSION - A Bill to direct the Federal Trade Commission to conduct a study on the governance of neural data and other related data, and for other purposes 2025

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance) 2025

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) 2024