Unlocking Neural Privacy: The Legal and Ethical Frontiers of Neural Data

March 13, 2025

Over the last quarter century, the boundaries of privacy have shifted dramatically. Once considered private, vast amounts of personal information about individuals – names, addresses, medical records, spending habits – have become commodified and, in some cases, widely accessible. For many, it feels as though the last frontier of privacy lies in the sanctity of our inner thoughts, emotions and feelings. However, rapid advancements in neurotechnology are now poised to challenge this assumption.

Neurotechnologies, including wearable devices, noninvasive interfaces and even implanted devices, are beginning to process "neural data" – information derived directly from the brain and nervous system. This data can reveal mental states, emotions and even intentions. As these devices move from research labs to consumers' hands, industries from healthcare and gaming to education and marketing are finding use cases for neural data that promise to revolutionize their sectors. Yet, this progress comes with significant ethical and legal questions.

Given the sensitive and unique nature of neural data, the stakes are high for businesses leveraging this technology. Not only must they navigate a patchwork of emerging regulations across jurisdictions, but also, they must consider the ethical dimensions of handling such personal and invasive information. This article explores the current state of the law on neural privacy, highlights emerging trends and suggests strategies for businesses looking to responsibly integrate neurotechnologies into their operations.

Neural data: What it is and why it's different

Neural data is unlike any other type of personal information. Where traditional data might describe a person (name, age, medical history), neural data can **reveal** the person. It serves as a kind of digital "source code" for an individual, potentially uncovering thoughts, emotions and even intentions. From EEG readings to fMRI scans, neural data allows insights into neural activity that could, in the future, decode neural data into speech, detect truthfulness or create a digital clone of an individual's personality.

The potential applications of neural data are staggering:

- Medical applications: Predicting epileptic seizures, treating paralysis or managing mental health conditions, such as depression and anxiety.
- Consumer applications: Enabling quadriplegic individuals to play video games or allowing drivers to control smart devices with thought alone.
- Commercial applications: Advertising based on emotional engagement, improving workplace productivity or tailoring educational experiences based on student focus.
- Public safety applications: Detecting fatigue in drivers or workers, aiding law enforcement investigations or identifying individuals through unique neural activity patterns.

While these developments hold extraordinary promise, they also underscore the critical need for safeguards. Neural data – due to its highly personal nature – is vulnerable to misuse, whether through commercialization, discrimination or outright breaches of privacy.

A nascent legal landscape: Neural privacy laws around the globe

The rapid development of neurotechnologies has outpaced regulatory frameworks in many jurisdictions. However, a few forward-looking regions have begun to address the unique privacy issues associated with neural data. Key developments include:

United States: State-led efforts

Colorado – Colorado became the first US state to explicitly include neural data under its definition of "sensitive personal information" in its comprehensive privacy law. The law imposes obligations, such as obtaining explicit consent for neural data collection, regularly refreshing that consent and conducting data protection assessments. However, ambiguities remain. For example, the law's definition of "biological data" limits its scope to information that is used or intended to be used to identify a person, leaving questions about the treatment of neural data for broader applications.

The Colorado law requires businesses to:

- Post a privacy notice informing individuals about their collection, use, retention and disclosure of this information, including each purpose for which each kind of personal information is used.
- Obtain clear, freely given, informed, specific, affirmative and unambiguous consent from an individual before collecting or using their neural data.
- Refrain from using dark patterns when obtaining consent from individuals.
- Refresh each individual's consent every 24 months, absent having interacted with the individual in the meantime, or provide a user-controlled interface for the individual to manage their opt-out preferences at any time.
- Inform individuals of the names of any third parties to which the business sells this information.
- Delete or de-identify this information when it is no longer necessary for the purpose for which it was collected, and in any event when an individual has withdrawn consent for its use.
- Inform individuals of the purposes for which it uses this data and only collect such information that is reasonably necessary to fulfill, or that is compatible with, those purposes, absent additional consent.
- Afford individuals the right and ability to access, correct and delete this information from the business's possession or control, and to opt out of the business selling this information or using it for targeted advertising or to make important automated decisions.
- Conduct data protection assessments on the collection, use, retention and disclosure of this information.
- Not use this data for unlawful discrimination.
- Take reasonable measures to secure this data.

California – A new law in California also classifies neural data as "sensitive personal information." Unlike Colorado's approach, California's law gives individuals a limited right to opt out of a business's collection and use of their neural data, instead of requiring businesses to receive consent from the individual first. On the other hand, the California law is broader than the Colorado law because it applies to employee data in addition to consumer data.

European Union: Data protection meets neurotechnology

- General Data Protection Regulation (GDPR): While the GDPR does not specifically address neural data, existing provisions related to biometric data and health data likely apply. Neural data collected for purposes like brain-computer interfaces or health monitoring may qualify as "special categories of data," requiring heightened safeguards such as explicit consent, transparency and proportionality in processing.
- Spain and the European Data Protection Supervisor (EDPS) report: The Spanish Data Protection Authority and the EDPS released a joint report on the implications of neurotechnology under EU data protection laws. The report highlights concerns about the accuracy, fairness and proportionality of neural data processing and emphasizes that businesses must assess these factors before deployment.

South America: Landmark constitutional amendment and ruling

In 2021, Chile became the first country in the world to amend its constitution to explicitly protect "neurorights." This development enshrines the mental privacy and integrity of individuals as fundamental rights, raising the bar for businesses operating in Chile to adopt a human rights-based approach to neural data.

In August 2023, the Chilean Supreme Court issued a landmark ruling against Emotiv, a US-based neurotechnology company, concerning its use of neural data collected through Emotiv's "Insight" device, a wireless EEG headset that collects neural data with the aim of interpreting emotions and executing mental commands. The plaintiff argued that Emotiv did not offer adequate privacy protection since users could have access to, or ownership of, their neural data only if they bought a paid license; otherwise, their data would remain in Emotiv's possession even if users deleted their accounts. Moreover, the plaintiff alleged, Emotiv's privacy policy stated that it had the right to transfer user data to third parties, which presumably included the sale of the plaintiff's data.

Since the plaintiff chose a free license, his neural data was not available to him, and he alleged that Emotiv had collected and used his neural data without explicit consent for unauthorized purposes. The Chilean Supreme Court ruled in favor of the plaintiff and ordered Emotiv to, among other things, delete the plaintiff's neural data and allow Chilean authorities to conduct strict assessments of its products prior to commercialization.

United Kingdom: Ethical and practical concerns

The UK Information Commissioner's Office (ICO) published a 2023 report titled, "Tech Futures: Neurotechnology," emphasizing the potential risks associated with neural data. It highlights issues such as the accuracy of neural data, transparency challenges and the risk of discrimination, particularly in artificial intelligence-powered neurotechnologies. The ICO urged businesses to adopt a precautionary approach to avoid misuse and ensure compliance with UK privacy laws.

The United Nations Educational, Scientific and Cultural Organization (UNESCO)

In August 2024, UNESCO appointed an internal expert group to prepare a new global standard on the ethics of neurotechnology. The framework is planned for adoption in November 2025 and aims to ensure that the use of neurotechnologies complies with human rights.

The path forward: Innovation with integrity

Neurotechnology is redefining what it means to collect and process personal information. Neural data is not just another category of personal information; it is a gateway to the most intimate aspects of who we are. As businesses harness the power of this technology, they carry the responsibility to use it ethically, transparently and in ways that respect individuals' rights.

The emerging legal frameworks surrounding neural privacy are just the beginning. By taking proactive steps to integrate privacy and ethical considerations into their operations, neurotech companies can lead not just in innovation but also in building trust and shaping a responsible future for the industry.

Key takeaways – What neurotech companies should do now

As neural privacy laws and ethical norms continue to evolve, businesses in the neurotechnology space can take several steps to ensure compliance and build consumer trust:

- **Conduct comprehensive privacy assessments.** Evaluate the risks and benefits of collecting neural data, taking into account the sensitive nature of this information.
- **Adopt privacy-by-design principles.** Embed safeguards into products and services from the earliest stages of development.
- **Stay ahead of regulatory developments.** Monitor emerging laws, such as those in California and Colorado, and adopt practices that exceed compliance thresholds to future-proof operations.
- **Engage stakeholders.** Partner with legal experts, ethicists and technologists to assess the societal implications of neural data applications.
- **Educate users.** Provide clear, accessible information about how neural data is collected, used and stored, empowering users to make informed choices.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Kristen Mathews New York	kmathews@cooley.com
Tania Soris Washington, DC	tsoris@cooley.com +1 212 479 6856

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.