Comparing New Neural Data Privacy Laws In 4 States

By **Kristen Mathews** (June 27, 2025)

Kristen Mathews

For the first time, businesses that develop or deploy neurotechnology must grapple with a rapidly materializing body of state legislation that regulates the collection, use, retention and disclosure of neural data.

In the past 14 months, Colorado, California and Montana, and most recently Connecticut, have each enacted statutes that treat neural data as a distinct — and sensitive — class of personal information.

Together, these laws signal a decisive shift away from the broad, tech-agnostic privacy statutes of the last decade and toward a new generation of requirements that specifically target brain-computer interfaces, wearable neuro devices, and other technologies capable of capturing and deriving information from electrical activity and blood circulation and oxygenation in the human nervous system.

At the same time, this moment presents an opportunity for neurotechnology companies to get in front of the regulatory curve by adopting robust self-regulatory practices, helping to shape the standards and expectations that will inform future laws.

Neural data raises unique privacy concerns because, when decoded by contemporary neurotechnology and machine learning techniques, it has the potential to infer sensitive insights about that person, including their mental and physical health conditions, emotions and stress levels, personality traits, propensity for risk-taking, and memories of specific stimuli.

Although no federal law yet addresses neural privacy in a comprehensive manner, the combined effect of Colorado H.B. 24-1058, California S.B. 1223, Montana S.B. 163 and Connecticut S.B. 1295 is already shaping the regulatory future.

And because the obligations are not identical, a multistate compliance strategy has quickly become a gating item for manufacturers, software developers, health technology platforms, consumer brands and employers experimenting with neuro-enabled workplace tools.

Below, we explain the core provisions of each statute, highlight the thematic overlaps and critical divergences, and offer practical steps companies can take now to mitigate risk while maintaining the speed of innovation.

The New Landscape: Comparing Colorado, California, Montana and Connecticut Neural Data Privacy Laws

Colorado, California, Montana and Connecticut have each enacted statutes that specifically regulate neural data, but their approaches differ in key respects.

Collectively, these laws define "neural data" as information generated by measuring the activity of an individual's nervous system, typically via devices such as brain-computer interfaces, neuro-headsets or EEG-enabled wearables. However, the scope, consent requirements and operational obligations vary across the three states.

Key Definitions and Scope

Neural Data

All four states define "neural data" as information generated by measuring nervous system activity, but Colorado includes it under the broader category of "biological data," which is limited to data used or intended for identification. Connecticut includes data from the central nervous system but not the peripheral nervous system.

Applicability

Colorado's and Connecticut's laws apply to any entity processing neural data, regardless of revenue or the number of individuals. California's law applies to businesses meeting California Consumer Privacy Act thresholds, and covers employee and business representative neural data. Montana's law applies broadly to any entity handling neural data of Montana residents, with no volume threshold.

Consent Models

Colorado and Connecticut require opt-in, affirmative consent before processing neural data, with a prohibition on dark patterns.

California adopts an opt-out model, allowing businesses to process neural data until a consumer exercises their right to limit use. However, an opt-out right is not required unless the data is used beyond specified purposes and to infer characteristics about the consumer.

Montana imposes the most granular, multilayered consent regime, requiring separate express consent for the collection, use, disclosure, transfer to third parties, secondary uses, research, marketing and sale of neural data.

Transparency and Notice

Colorado requires a privacy notice specifying each purpose for which neural data is used and all categories of third-party recipients.

California mandates notice at the point of collection, including categories of neural data, purposes, retention periods, and whether data will be sold or shared for cross-context behavioral advertising.

Meanwhile, Montana requires two separate notices — a high-level privacy policy overview and a detailed, publicly available privacy notice covering collection, use, access, security, retention and deletion practices.

And in Connecticut, in addition to the typical requirements, the privacy notice must contain a statement disclosing whether the controller collects, uses or sells personal data, including neural data, for the purpose of training large language models.

Data Subject Rights

All four states provide individuals with rights to access, correct, delete, and (in most cases) port their neural data and allow consumers to opt out of sales and targeted advertising.

Data Localization and Storage

In all four states, businesses must take measures to maintain the security of neural data.

Montana stands out by prohibiting storage of neural data in countries sanctioned by the U.S. or designated as foreign adversaries, and requires consumer consent for storage or transfer outside the U.S.

Colorado, California and Connecticut do not impose data localization requirements specific to neural data.

Impact Assessments

In Colorado, California and Connecticut, businesses must conduct privacy impact assessments regarding their handling of neural data.

Special Considerations

Health Insurance Portability and Accountability Act Carveouts

Montana provides a partial exemption for HIPAA-covered entities, but only if separate informed consent is obtained for neural data and consumers are given access, deletion and opt-out rights outside clinical trials. Colorado, California and Connecticut generally exempt HIPAA-regulated data.

Government Access

Montana requires a search warrant or subpoena based on probable cause for government access to neural data, unless the individual has waived privacy rights.

Data Sharing

Montana prohibits a business from disclosing a consumer's neural data to any entity offering health insurance, life insurance or long-term care insurance, or to the consumer's employer, absent the consumer's express consent.

Operational Takeaways

The patchwork of requirements means that businesses must carefully map data flows, design unified consent experiences and implement layered privacy notices to comply across

jurisdictions.

Montana's law, with its detailed consent and localization mandates, sets the high-water mark for compliance programs. Meanwhile, California's opt-out regime and Colorado's requirement to refresh consent every 24 months require nuanced operational controls and ongoing risk assessments. Connecticut's definition of neural data is narrower than the others.

Themes, Contrasts and Compliance Triage

Issue	Colorado	California	Montana	Connecticut
Consent model	Opt-in	Limit-use opt-out	Multilayer express opt-in	Opt-in
Workforce data	Exempt	Covered	Covered	Exempt
Applicability thresholds	None for neural/biological data	CCPA thresholds	No volume threshold	No volume threshold
Data localization	None	None	U.S. storage mandated unless consumer consents	None
Enforcement	AG	AG + CPPA + private right for data breaches	AG	AG

Defining the Universe: Gaps and Overlaps in Neural Data Regulation

The current wave of neural data privacy laws attempts to regulate the space by first defining a universe of covered data — neural data — and then imposing requirements on businesses that collect, use or disclose that data. However, these definitions are both overbroad and underinclusive in important ways.

For example, the laws focus on data generated by measuring the activity of the central or peripheral nervous system, but leave out other types of biological data — such as heart rate or eye movement — that can also be used to infer a person's feelings, mental states or intentions. As a result, businesses that use technologies capable of deriving sensitive cognitive or emotional information from nonneural signals may fall outside the scope of these statutes, even though the privacy risks may be similar.

Conversely, some neurotechnologies may collect data from the nervous system that is technically covered by the law, even if the technology is not actually being used to derive cognitive or emotional information about the individual. This means that businesses may be subject to regulatory obligations even when the societal concerns that motivated these laws are not present.

Notably, the Connecticut law defines "neural data" as data derived from the central nervous system, excluding the peripheral nervous system, likely because the legislators considered data from the latter to be less sensitive.

Looking ahead, future legislation may move toward regulating the uses of cognitive or affective data that raise societal concerns, rather than all neural data regardless of context.

In the meantime, neurotechnology businesses have an opportunity to lead by example — crafting self-regulatory frameworks that focus on the responsible use of technologies capable of deriving sensitive information about individuals. By developing standards that are practical for businesses, protective of individuals and responsive to societal values, the industry can help shape the next generation of neural privacy regulation in a way that works for everyone.

In addition to these U.S. state laws, several countries in Europe and South America have taken significant steps to protect neural privacy at the national level. For example, Chile was the first to recognize a neural privacy right when it amended its constitution to explicitly safeguard neurorights and mental privacy.

Other countries have enacted laws, or are actively considering or drafting legislation to regulate neural data, signaling a growing global consensus around the need for robust protections in this area.

Building a Cohesive, Multistate Compliance Program

Because the four statutes are structurally similar but procedurally distinct, a highest-common-denominator strategy often yields the most efficient path.

Data Mapping and Classification

Inventory every data flow that touches brain-signal outputs (EEG, fNIRS, EMG, ECoG, heart rate variability used for mental-state inferences). Flag whether the signals are linked, or reasonably linkable, to an identified person.

Unified Consent Experience

Design a single onboarding sequence that meets Montana's granular permissions while satisfying Colorado's and Connecticut's opt-in and California's notice at collection. Offer checkbox granularity for research, marketing and sale to ensure modular withdrawal. Enable consumers to change their preferences any time.

Dynamic Privacy Notices

Implement layered notices: a concise mobile splash screen (Montana's overview; California's notice at collection) plus a full-length policy accessible in-app and on the web. Incorporate drop-down menus to reflect evolving use cases.

Data Protection Assessments

Adopt a generic assessment template as the baseline, then add localization risk analysis (Montana) and purpose-limitation justifications. Refresh annually or upon a material change.

Vendor and Research Agreements

Insert neural-data-specific rider clauses: delineating processor/third-party status, restricting secondary use, imposing subprocessor flow-downs and addressing extra-U.S. storage prohibitions. Maintain a public list or readily accessible portal naming each third-party recipient of neural data.

User Rights Portal

Build or license a rights management interface that accommodates access, correction, deletion, portability, opt-out of sale/sharing, and localized storage consents. Automate verification flows to reduce latency.

Security Controls and Audits

Align technical safeguards with National Institute of Standards and Technology Special Publication 800-53 or International Organization for Standardization 27001 series, layering encryption of raw neural signals at rest and in transit, and implementing role-based access control to decouple identity keys from neural patterns.

The Road Ahead

State lawmakers are openly signaling that neural privacy is the next biometrics-style frontier. Illinois has already proposed adding neural data to the Biometric Information Privacy Act, and 14 states have neural data bills pending. Businesses that wait and see risk retrofitting products at considerable cost, or worse, halting deployments pending compliance retrofits.

The emergence of Colorado, California, Montana and Connecticut's neural privacy statutes represents a pivotal moment for neurotechnology: The law is now evolving at nearly the same pace as the science.

Companies that proactively operationalize consent, transparency and security will not only avoid regulatory turbulence but also earn the confidence of consumers, clinicians, employees and investors who are understandably cautious about technology that touches the literal core of human identity.

By leading with strong self-regulation and ethical practices, neurotechnology companies can help shape the future legal landscape, demonstrating industry leadership and influencing the standards that lawmakers may ultimately adopt.

In short, compliance is no longer a post-commercialization bolt-on; it is a strategic imperative that must sit at the whiteboard with product design, engineering and business development from day one.

Kristen Mathews is a partner at Cooley LLP.