Cooley

From Maple to Mind Taps: New Vermont Law Puts Neurotech on Notice

June 23, 2026

Vermont, a state famous for tapping maple trees, is now tapping into something far more complex: the human brain. With the enactment of S.71, the Vermont Data Privacy and Online Surveillance Act, the Green Mountain State has become the fifth state in the nation (after California, Colorado, Connecticut and Montana) to classify "neural data" as "sensitive data" subject to the most stringent privacy protections under state law. For the rapidly expanding consumer neurotech industry – from EEG-enabled meditation headbands and neurofeedback wearables to emerging brain-computer interfaces – the law imposes consent requirements, purpose limitations and assessment obligations that impact how companies collect, use and monetize the data generated by measuring the activity of the human brain. Crucially, the law contains no revenue threshold, meaning even early-stage startups processing neural data from as few as 3,000 consumers will find themselves subject to its full reach. However, the law contains exceptions for HIPAA protected health information, healthcare components of HIPAA covered entities and HIPAA business associates. Neurotech companies who make their products available to patients through the healthcare system might enjoy one of these exceptions.

What is neural data under the act?

The act defines "neural data" as "any information that is generated by measuring the activity of an individual's central nervous system." This broad definition is technology-neutral and captures data from a range of consumer neurotechnology devices and applications, including electroencephalography (EEG) headsets, neurofeedback devices and emerging brain-computer interface technologies. At the same time, Vermont's definition is narrow relative to the other four states except Connecticut, because the definition references the central nervous system but not the peripheral nervous system.

The act classifies neural data as a category of "sensitive data," placing it alongside other specially protected categories that include biometric data, genetic data, precise geolocation data, consumer health data, data revealing racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, and data concerning mental or physical health conditions. This classification subjects neural data to the act's most restrictive requirements for collection, processing and sale.

Who does the law apply to? A low bar for emerging companies

The act's applicability thresholds are notable for what they do not require: revenue. Unlike some state privacy laws that apply only to businesses meeting certain revenue benchmarks, Vermont's law is triggered by data volume alone. A company falls within the act's scope if, during the preceding calendar year, it meets any one of three independent thresholds:

- Controlled or processed the personal data of not fewer than 35,000 consumers (excluding data processed solely for completing a payment transaction).
- Controlled or processed the **sensitive data** (such as neural data) of not fewer than **3,000 consumers** (excluding data processed solely for completing a payment transaction).
- Offered for sale in trade or commerce the personal data of not fewer than 3,000 consumers.

Because neural data is classified as sensitive data, the second threshold is the critical one for the neurotech industry. A pre-revenue wearable neurotech startup that has distributed devices to 3,000 consumers and collects neural data from those users would be subject to the full weight of the act's obligations – regardless of the company's size, stage, revenue or financial resources. This means that new and emerging companies in the

business-to-consumer neurotech space cannot assume the law does not apply to them simply because they are small or have limited revenue. This makes the new Vermont law similar to the Connecticut law passed around the same time last year, which applies to any business that processes sensitive personal data regardless of revenue or volume of data.

Consent is required – but it is not a blank check

Under the act, a company may not process sensitive data, including neural data, "unless the consumer has provided consent and unless the processing is reasonably necessary in relation to the purposes for which the sensitive data are collected."

This two-part test imposes a meaningful constraint that goes well beyond a simple notice-and-consent model. Even where a consumer has affirmatively consented to the collection of neural data – for example, in connection with a meditation, focus-training or cognitive wellness application – the company may only use that data for purposes that are "reasonably necessary" in relation to the specific purposes for which it was originally collected.

The "consent" required by the act is itself defined with precision. "Consent" means "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer." Consent does not include acceptance of general or broad terms of use, hovering over or closing content, or agreement obtained through the use of dark patterns.

The practical implication is significant. A neurotech company that collects neural data to provide a brain wellness or cognitive performance service cannot repurpose that same data for unrelated secondary uses – such as generating advertising insights, training third-party AI models, licensing data to pharmaceutical researchers or developing entirely new product lines – even if it has obtained the consumer's consent to collect the data in the first instance, unless the additional uses meet the "reasonably necessary" standard. The "reasonably necessary" standard effectively prevents consent from operating as a blank check for unlimited downstream processing. A company may still de-identify data and use de-identified data for secondary purposes, but to do so it would need to effectively de-identify the data in a way that satisfies the law's de-identification standards.

This limitation has the potential to directly disrupt the business models of consumer neurotech companies that rely on secondary data monetization as a revenue stream. Companies that have built financial projections around the ability to leverage neural data beyond their primary service offering – for example, by licensing aggregated neural response patterns to advertisers or by using neural engagement data to optimize third-party content – will need to reassess those assumptions in light of the act's purpose-limitation framework.

Perhaps the most consequential open question under the act – and the question that every neurotech business will be grappling with – is where, exactly, the line falls on the "reasonably necessary" standard. Consider a neurotech company that collects neural data to power a focus-training application. If that company uses the neural data it collects to train its own AI models to improve the accuracy and performance of that same focus-training product, is that use "reasonably necessary in relation to the purposes for which the sensitive data are collected?" There is a credible argument that it is: Improving the core product the consumer signed up for through machine learning could be viewed as integral to the very service for which the data was collected. But the act does not explicitly address this question, and the answer may ultimately depend on how broadly or narrowly the attorney general and the courts interpret the required nexus between AI training and the consumer-facing service.

A far more difficult question arises when a company attempts to expand the boundaries of "reasonably necessary" by defining its collection purposes broadly at the outset. Could a neurotech company inform consumers at the point of collection that one of the purposes for which it is collecting their neural data is to license it to third parties, use it for targeted advertising or train external AI models – and then argue that these uses are "reasonably necessary in relation to the purposes for which the sensitive data are collected" because they were disclosed as purposes from the very beginning? Neurotech companies exploring this strategy should proceed with the advice of experienced privacy counsel.

No sale of neural data without consent

The act separately prohibits the sale of sensitive data, including neural data, unless the consumer has provided consent. This prohibition applies independently of, and in addition to, the consent required for processing data. For neural data, any transfer to a third party in exchange for monetary or other valuable consideration requires its own affirmative consumer consent.

The act defines "sale of personal data" as "the exchange of a consumer's personal data by the company with a third party for monetary or other valuable consideration." Certain disclosures are excluded from the definition of a sale, including disclosures to a processor acting on the company's behalf, disclosures to affiliates, disclosures directed by the consumer and transfers in connection with a merger or acquisition. However, the core commercial sale of neural data to third parties for their independent use will require consent.

Mandatory data protection assessments

The act requires companies to "conduct and document a data protection assessment" for each processing activity that presents "a heightened risk of harm to a consumer." The processing of sensitive data, which expressly includes neural data, is specifically enumerated as one such heightened risk activity.

Each assessment must identify and weigh the benefits that may flow from the processing – to the company, consumer, other stakeholders and the public – against the potential risks to the rights of the consumer, as mitigated by safeguards the company can employ. The company must also factor in the use of deidentified data, the reasonable expectations of consumers and the context of the processing relationship.

For neurotech companies, this means that before processing neural data, they must prepare a formal, documented assessment analyzing the risks and benefits of each neural data processing activity. These assessments are not merely internal paperwork; the attorney general may require a company to disclose any data protection assessment relevant to an investigation, and the attorney general may evaluate the assessment for compliance with the act. While the assessments are confidential and exempt from public records disclosure, companies should prepare them with the understanding that they may be reviewed by enforcement authorities.

The data protection assessment requirements apply to processing activities created or generated after January 1, 2028, and are not retroactive.

Enforcement and timeline

The act takes effect on **January 1, 2028.** A violation of the act is deemed a violation of the Vermont Consumer Protection Act, enforceable by the attorney general. Notably, the act does not create a private right of action for consumers, although it leaves open the possibility for the legislature to add one if the attorney general is not given adequate funding and resources to enforce the law.

During a transitional period from January 1, 2028, through June 30, 2029, the attorney general must issue a notice of violation 60 days before initiating an enforcement action, provided the attorney general determines that a cure is possible. A controller or processor of data that receives such a notice has 60 days to cure the violation. After June 30, 2029, the attorney general is no longer required to provide a cure opportunity before bringing an enforcement action.

The General Assembly has also directed that the attorney general provide, and update as necessary, guidance to companies for compliance with the act.

The 'other' Vermont neural rights law

The Vermont Legislature separately enacted H.814, titled "An act relating to neurological rights and the use of artificial intelligence technology in health and human services," which was adopted on May 18, 2026 – roughly a month before S.71. Despite its ambitious original billing, H.814 lost its teeth during the amendment process. As introduced, the bill proposed to create enforceable privacy standards for neural data and prohibit electronic devices from bypassing an individual's conscious decision-making without consent. By the time it was adopted, however, all of those operative provisions had been stripped out.

What remains is an aspirational statement “recognizing” that individuals have rights to mental and neural data privacy, freedom of thought and protection from neurotechnological interventions – but without any enforcement mechanism, compliance obligations, consent requirements or penalties for businesses. The bill’s only operative substance is a directive to Vermont’s Artificial Intelligence Advisory Council to study the issues and report back to the legislature by January 15, 2027, with recommendations for future protections and proposed definitions. In short, H.814 is a study bill, not a regulatory one. It creates no new obligations for neurotech companies and requires no action. S.71, discussed above, is the law that demands attention and compliance planning.

Key takeaways for neurotech companies

1. **Assess whether you are in scope.** Any company that processes neural data from 3,000 or more Vermont consumers in a calendar year is subject to the act, regardless of revenue, company size or stage of development.
2. **Obtain proper consent.** Consent for processing neural data must be a clear affirmative act that is freely given, specific, informed and unambiguous. Buried terms-of-use provisions or dark-pattern-driven consent flows will not satisfy the act’s requirements.
3. **Audit your data uses against the purpose-limitation standard.** Even with valid consent, neural data may only be processed for purposes reasonably necessary in relation to the purposes for which it was collected. Secondary monetization strategies – advertising insights, third-party AI training, data licensing – that are untethered to the primary service must be risk tolerant.
4. **Prepare for the sale consent requirement.** Any sale of neural data to third parties for monetary or other valuable consideration requires separate consumer consent.
5. **Conduct and document data protection assessments.** Before processing neural data, prepare a formal assessment weighing the benefits against potential risks to consumers. These assessments may be reviewed by the attorney general in the context of an investigation.
6. **Reevaluate business models built on secondary neural data monetization.** The act’s purpose-limitation framework may foreclose revenue streams that depend on repurposing neural data beyond the service for which it was originally collected. Companies should assess their data practices and adjust their business strategies well in advance of the January 1, 2028, effective date.

Key Contacts

Kristen Mathews **New York**	**kmathews@cooley.com**