Cooley

Your Brain, Their Rules: The Growing Patchwork of Neural Data Regulation

February 24, 2026

According to one study, investment in the global neurotechnology market is projected to increase to more than $50 billion by 2034. While this technology promises to revolutionize human existence in a number of ways, legislators are taking note of its rapid advancement. In the first six weeks of 2026, nine bills that would regulate neural data to varying degrees have been introduced across six US states, including Alabama, California, Illinois, New York, Vermont and Virginia (2026 neural data bills). One of these bills applies exclusively to government entities. This is in addition to several other bills addressing neural data that were introduced in 2025 and are still working their way through the legislative process.

In this survey, we provide an overview of the key themes of the 2026 neural data bills to highlight issues that businesses innovating in neurotechnology should be thinking about as the regulatory landscape in this area evolves. We also provide a detailed breakdown of each proposed bill, including key definitions, applicability, obligations and enforcement.

Key themes of the 2026 neural data bills

As neurotechnology shifts from research to commercial reality, companies will need to consider a host of new requirements regulating neural data. Neural data is arguably one of the most sensitive types of personal information, offering direct and unfiltered insight into an individual’s cognitive and emotional state. While some scholars describe neural data as the final frontier of privacy, for many companies, neural data represents the next frontier in data regulation. Below we outline key issues that organizations will need to think about and that feature as common themes across the 2026 neural data bills.

1. Developing taxonomies of neural data

In contrast to other laws regulating personal information where many forms of data share standard definitions, legislators have not yet converged on a uniform definition of neural data. While definitions of neural data in the 2026 neural data bills generally center on information that is generated by measuring the activity of an individual’s central or peripheral nervous system, a closer read of the definitions highlights important nuances. For example, Illinois SB 2994 and New York AB 10008 and SB 9008 carve out nonneural information from their definitions. The Illinois bill provides additional color as to what constitutes nonneural information (i.e., pupil dilation, motor activity, breathing rate and other information about the downstream physical effects of neural activity), while the New York bills are silent as to what nonneural information is. Virginia HB 654 builds the definition of neural data into the existing definition of biometric data under the Virginia Consumer Data Protection Act (VCDPA). Vermont HB 814 introduces ancillary neurotechnology terms, such as “brain-computer interface,” “conscious decision making” and “conscious bypass.” Companies will need to carefully examine neural data laws to understand the finer details of the definitions and how they may apply to their neurotechnology.

2. Consent is key

Unsurprisingly, given the sensitive nature of neural data, the 2026 neural data bills generally require companies to obtain consent from individuals before processing neural data. The type of processing that requires consent with respect to neural data differs among the bills, but it is clear that legislators intend for individuals to be firmly in control of the collection, storage and disclosure of their neural data. Companies should implement procedures for obtaining consent from individuals that interact with their neurotechnologies and have protocols in place to respond if a consumer withdraws that consent. Certain of the proposed laws, such as Illinois HB 5179 and Vermont HB 814, require deletion of neural data within specified time frames upon revocation of consent.

3. Transparency ensures accountability

Many of the 2026 neural data bills require companies to provide transparency around how they will process neural data. The disclosure obligations vary widely among the proposed laws. For example, Illinois SB 2994 requires covered entities to provide clear and complete information regarding a covered entity's policies and procedures for the collection, use and disclosure of neural data, while Alabama HB 263 requires a covered entity that transfers, discloses or uses a consumer's neural data for certain purposes to notify the consumer before engaging in these activities and provide the consumer the opportunity to limit or prevent the processing of their neural data. Illinois HB 5179 requires companies to disclose certain information about neural devices, including health and safety risks associated with the use of a neural device and whether the neural device collects data in addition to whatever data collection is necessary to perform the advertised or described function of the neural device, among other items.

4. Broad regulation and sector-specific rules

Companies will need to account for the broad reach of neural data laws, some of which amend existing privacy laws and apply to many data activities, while navigating sector- and entity-specific laws. For instance, Virginia HB 654 amends the VCDPA to expand the definition of "biometric data" to include "neural data," which in turn extends broader restrictions on the processing of "sensitive data" to "neural data." Illinois SB 2994 amends existing obligations under the Illinois Genetic Information Privacy Act (GIPA), but these requirements are specific to insurers and employers with respect to their use of neural data for certain activities. At the same time, SB 2994 introduces additional obligations on organizations that offer neurotechnology products or collect, use and analyze neural data. NY AB 10008 and SB 9008 apply to data brokers that may process neural data. Companies innovating in neurotechnology will, therefore, need to carefully examine the reach of neural laws applicable to them and consider the industry they operate in as part of a sound compliance strategy.

5. Enforcement regimes vary

The 2026 neural data bills take differing approaches to enforcement, with state attorneys general serving as the primary enforcement body for the majority of the bills with the ability to bring actions in court. Some of the proposed laws, such as Illinois SB 2994 and HB 5179 and Vermont HB 814, provide individuals with a private right of action. Similar to state biometric privacy laws, companies will need to assess the risk of collecting and processing neural data from specific states where enforcement regimes are more stringent.

We provide below a detailed breakdown of the requirements discussed above. Importantly, these 2026 neural data bills are not the first laws on the books to regulate neural data. Colorado, California, Montana and Connecticut have enacted statues regulating neural data as a distinct category of personal information. For more information, see Cooley's July 2025 article, "Comparing New Neural Data Privacy Laws in Four States." As mentioned above, there are several other bills addressing neural data that were introduced in 2025 and are still going through the legislative process. For more information, see this "Neurotech Laws and Legislation Update."

2026 neural data bills in detail

1. Alabama HB 263

Summary: Alabama HB 263 prohibits a covered entity from disclosing, transferring or taking certain other actions with regard to a consumer's biological data or neural data without the consumer's express consent.

Key definitions: HB 263 defines "biological data" as "data generated by (i) the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological or neural properties, compositions, or activities; or (ii) an individual's body or bodily functions, which are used or intended to be used for identification purposes." "Neural data" is defined as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous system and that can be processed by or with the assistance of a device." A "consumer" is any individual who is an Alabama resident.

Application: HB 263 applies to any individual or entity that maintains, owns or licenses biological data or neural data in the course of the individual's or entity's business, vocation or occupation.

Obligations: HB 263 provides that a covered entity may not:

- Transfer a consumer's biological or neural data to a third party.
- Disclose a consumer's biological or neural data to a third party for a reason other than fulfillment of the entity's products or services.
- Use a consumer's biological or neural data for a purpose other than what is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests the goods or services.
- Market to a consumer based on their biological or neural data.

HB 263 further provides that if a covered entity transfers, discloses or uses a consumer's biological or neural data for purposes other than those described above, it must, before the transfer, disclosure or use, notify the consumer and provide the consumer the opportunity to limit or prevent the transfer, disclosure or use.

Enforcement: Consumers can report any violation of HB 263 to the Consumer Interest Division in the Alabama Attorney General's Office, and the attorney general may bring an action in court to enjoin conduct or practices that violate the act and seek a civil penalty of up to $3,000 for each violation.

Effective date: If passed and ultimately signed into law, HB 263 would become effective on October 1, 2026.

2. California AB 1883

Summary: California AB 1883 amends the California Labor Code and introduces restrictions on employers' use of workplace surveillance tools, including collection of neural data through such tools.

Key definitions: AB 1883 defines "neural data" as "information that is generated by measuring the activity of a worker's central or peripheral nervous system, and that is not inferred from nonneural information." AB 1883 defines a "workplace surveillance tool" to mean "any system, application, instrument, or device that collects or facilitates the collection of worker data, activities, communications, actions, biometrics, or behaviors, or those of the public that are also capable of passively surveilling workers, by means other than direct observation by a person, including, but not limited to, video or audio surveillance, continuous incremental time-tracking tools, geolocation, electromagnetic tracking, photoelectronic tracking, or that utilizes a photo-optical system or other means."

Application: AB 1883 applies to "employers," which are defined as "a person or governmental entity that directly or indirectly, or through an agent or any other person, employs or exercises control over the wages, benefits, other compensation, hours, working conditions, access to work or job opportunities, or other terms or conditions of employment, of any worker, including all branches of state government, or the several counties, cities and counties, and municipalities thereof, or any other political subdivision of the state, or a school district, or any special district, or any authority, commission, or board or any other agency or instrumentality thereof."

Obligations: AB 1883 prohibits employers from using a workplace surveillance tool that:

1. Prevents compliance with labor, occupational health and safety, employment and civil rights laws or regulations.
2. Identifies, profiles or infers information about workers engaging in activity protected by law.
3. Incorporates certain technologies, including emotion, facial or gait recognition technology or neural data collection.

Enforcement: AB 1883 is enforced by the Division of Labor Standards Enforcement through the labor commissioner. Public prosecutors may also bring civil actions to enforce the law, and workers have a private right of action. An employer who violates the law may be subject to a penalty of up to $500 per employee for each violation. For the same violation, recovery can constitute a statutory penalty paid to the employee or a civil penalty, but not both.

Effective date: AB 1883 is silent as to its effective date.

3. Illinois SB 2994

Summary: Illinois SB 2994 amends the IL GIPA to extend its protection to neural data, characterized in the bill as "neurotechnology data." GIPA was originally enacted in 1998 to govern confidentiality and use of genetic testing and genetic information by employers and insurers. SB 2994 introduces new restrictions to:

1. Prohibit insurers from using neurotechnology data for nontherapeutic purposes or underwriting, subject to limited exceptions.
2. Prohibit employers, employment agencies, labor organizations and licensing agencies (collectively, "employers") from requesting, requiring or using neurotechnology data in employment decisions, subject to certain exceptions.
3. Impose requirements on a separate category of covered entities to maintain the confidentiality of neurotechnology data.

Key definitions: SB 2994 defines "neurotechnology" as "devices capable of recording, interpreting, or altering the response of an individual's central or peripheral nervous system to its internal or external environment." Neurotechnology includes mental augmentation or improving human cognition and behavior through direct recording or manipulation of neural activity by neurotechnology. SB 2994 defines "neurotechnology data" as "information that is captured by neurotechnologies, that is generated by measuring the activity of an individual's central or peripheral nervous system, or that is data associated with neural activity, the activity neurons or glial cells in the central or peripheral nervous system." It does not include nonneural information, such as pupil dilation, motor activity, breathing rate or other information about the downstream physical effects of neural activity.

Application: SB 2994 applies to insurers, employers and covered entities. A covered "entity" means a partnership, corporation, association, or public or private organization of any character that offers consumer neurotechnology products or services directly to a consumer, or collects, uses or analyzes neurotechnology data.

Obligations: With respect to insurers, SB 2994 generally prohibits insurers from collecting, using, sharing or relying on neurotechnology data when making decisions about accident and health insurance, including for underwriting purposes. For instance, insurers can't ask individuals to provide such data, and if insurers receive such data, they can't use it for nontreatment purposes. If an individual voluntarily provides neurotechnology data, and the data is favorable to the individual, the insurer may consider it. Moreover, companies providing direct-to-consumer neurotechnology are prohibited from sharing any neurotechnology data about a consumer with any health or life insurance company without written consent from the consumer.

With respect to employers, SB 2994 restricts the use of neurotechnology data to make certain decisions. In particular, employers are prohibited from:

1. Soliciting, requesting, requiring or purchasing neurotechnology data of an individual or their family member.
2. Requiring an individual to use neurotechnology as a condition of employment, compensation or benefit.
3. Making decisions about the terms, conditions or privileges of employment or a preemployment application by relying on neurotechnology data.
4. Providing differential treatment to employees on the basis of their neurotechnology data.

With respect to covered entities, SB 2994 imposes a broad range of obligations. For instance, entities must disclose their policies and procedures for the collection, use and disclosure of neurotechnology data. They also must obtain consent for such processing of neurotechnology data, including separate express consent for the transfer of neurotechnology data to third parties other than the covered entity's processors, and for the use of such data beyond the primary purpose of the entity's neurotechnology product or service and inherent contextual uses. Express consent is required for marketing to a consumer based on their neurotechnology data, selling the consumer's neurotechnology data, or marketing by a third party to a consumer based on the consumer having ordered or purchased a neurotechnology product or service. SB 2994 also requires covered entities to develop, implement and maintain a comprehensive security program to protect a consumer's neurotechnology data against unauthorized access, use or disclosure, and must further provide a process for consumers to access their neurotechnology data, request and obtain destruction of such data, and revoke their consent, among other requirements.

Enforcement: GIPA provides individuals with a private right of action with damages of $2,500 or actual damages (whichever is greater) for negligent violations and damages of $15,000 or actual damages (whichever is greater) for intentional or reckless violations.

Effective date: If passed and ultimately signed into law, SB 2994 would enter into effect on January 1, 2027.

4. Illinois HB 5179

Summary: Illinois HB 5179, or the "Protection of Neural Data Act," imposes disclosure and consent requirements on an entity's use of a neural device to monitor, record, analyze or manipulate the neural data of an individual.

Key definitions: HB 5179 defines "neural data" to mean "information that (1) concerns the activity of an individual's central nervous system or peripheral nervous systems, including the brain and spinal cord, and (2) can be monitored, recorded, analyzed or manipulated by a neural device." A "neural device" means a "device that (1) employs an electronic, optical, magnetic, nanophysical, acoustical, or mechanical system and (2) is capable of replacing, restoring, complementing, improving, or otherwise modifying the response of the individual's central nervous system to its internal or external environment."

Application: HB 5179 applies to covered entities. A "covered entity" is defined as "a person that uses or facilitates the use of a neural device to monitor, record, analyze or manipulate the neural data of an individual. Individuals licensed in Illinois to provide healthcare services and that use such a neural device for a medical purpose and licensed healthcare facilities are not considered covered entities subject to the law.

Obligations: HB 5179 imposes disclosure and consent requirements on covered entities. Specifically, before using or facilitating the use of a neural device to monitor, record, analyze or manipulate the neural data of an individual, a covered entity must:

1. Plainly disclose on its website, if any, all user agreements, privacy agreements and other terms that the covered entity requires an individual to consent to in order to use the covered entity's neural device.
2. Plainly disclose:
   a. All health and safety risks associated with use of the neural device.
   b. Whether the neural device collects data in addition to whatever data collection is necessary to perform the advertised or described function of the device.
   c. That the covered entity may not store the individual's neural data after the individual's use of the neural device unless it has obtained the individual's consent.
   d. That the covered entity may not transfer possession of the individual's neural data to any third party unless the covered entity acquires the individual's consent.
   e. How the covered entity safeguards the privacy of individuals' neural data.

With respect to consent requirements, a covered entity may not store, retain or transfer an individual's neural data unless it obtains the individual's consent. Consent can be withdrawn at any time by the individual, and the covered entity must then promptly block any potential future transfer of the individuals' neural data to any third party, and within 30 days after the individual withdraws consent, must delete all neural data of the individual and contact each third party to which the covered entity transferred the individual's neural data and instruct the third party to delete the neural data. The third party that receives this instruction must promptly comply with it.

Enforcement: HB 5179 is enforceable by the Illinois attorney general and states attorneys. Violations of HB 5179 constitute a class 1 misdemeanor, and if a court identifies a pattern of noncompliance, it may impose a fine of up to $50,000 on the covered entity. HB 5179 also provides individuals with a private right of action. If a covered entity unlawfully transfers an individual's neural data to a third party in violation of the act, the individual is presumed to have suffered at least $10,000 in damage. The attorney general may also adopt rules necessary to implement HB 5179.

Effective date: HB 5179 is silent as to its effective date.

5. **New York AB 10008 and SB 9008**

Summary: New York AB 10008 and SB 9008 are companion bills in the New York Legislature for the 2025 – 2026 session to enact a comprehensive state budget package and introduce legal reforms across a number of areas. Regulation of neural data falls under the proposed amendment to the New York General Business Law, introducing the Data Broker Accountability Act (DBAA), which is identical across the companion bills. The DBAA includes a wide range of definitions, many of them similar to those found in the California Consumer Privacy Act (CCPA) and other comprehensive state privacy laws, but its substantive requirements only apply to data brokers. Neural data is a subset of sensitive personal information. The obligations applicable to data brokers with respect to personal information (which subsumes sensitive personal information), by extension, encompass neural data.

Key definitions: The DBAA defines a "data broker" as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom such business either (i) does not have a direct relationship and/or (ii) does not have a direct relationship with such consumer as to personal information it sells about such consumer that it collected outside of a consumer-facing business with which the consumer intends and expects to interact." "Sensitive personal information" means personal information that reveals, among other items, a consumer's neural data, meaning "information that is generated by measuring the activity of such consumer's central or peripheral nervous system, and that is not inferred from nonneural information."

Application: While the DBAA includes a definition of a "business" that largely tracks the CCPA's definition, in its current form, the obligations only apply to data brokers.

Obligations: The DBAA requires data brokers to register with the New York Department of Financial Services (NYDFS), respond to consumer deletion requests and disclose the number of deletion requests, among other items. The DBAA also requires NYDFS to establish an accessible deletion request mechanism, and data brokers must access the mechanism at least every 45 days and process requests and delete personal information related to consumers that submitted requests. While the DBAA does not include unique requirements specific to neural data, neural data is a subset of "sensitive personal information," which forms part of the definition of "personal information," and the obligations outlined above apply to "personal information."

Enforcement: The DBAA provides the superintendent of NYDFS with broad investigatory powers, and if a company violates the law, the superintendent can impose fines, including $200 per day for failing to register as a data broker, $200 per day per deletion request if the company fails to delete data when required, and $200 per day for failing to meet website disclosure requirements.

Effective date: If passed and ultimately signed into law, the DBAA takes effect 180 days after NYDFS issues implementing regulations.

6. Vermont HB 814

Summary: Vermont HB 814 provides neurological rights to individuals by creating privacy standards for neural data and by prohibiting electronic devices from bypassing the conscious decision-making of individuals who have not provided consent. Separately, HB 814 regulates certain aspects of artificial intelligence (AI) in health and human services, including mental health chatbots, use of generative AI in patient communications and use of AI in utilization review.

Key definitions: HB 814 defines "neural data" to mean "information that is generated by the measurement of the activity of an individual's central or peripheral nervous system and that can be processed by or with the assistance of a device." In contrast to the other bills, HB 814 provides some additional definitions specific to the neurotechnology context. HB 814 defines "brain-computer interface" (BCI) as a "device that enables its users to interact with a computer by means of brain activity only." "Conscious decision making" means "an individual making a deliberate decision with awareness and intention," and "conscious bypass" means "the use of neurotechnology to manipulate brain activity by applying electrical or optical stimuli without the conscious awareness of the individual whose brain activity is being manipulated."

Application: HB 814 applies to any "person," which is defined under the Vermont state statutes and includes a corporation.

Obligations: HB 814 prevents a person from collecting or recording an individual's neural data gathered from a BCI unless the person provides the individual with notice explaining how it will use the individual's neural data and subsequently receives written informed consent from the individual to collect or record their neural data. It also prevents a person from sharing with a third party an individual's neural data unless the person provides the individual with a written request for the individual's neural data to be shared with a third party and for what purposes, including the name and address of the third party, and subsequently receives written informed consent from the individual to share the individual's neural data. Individuals can revoke their consent at any time.

HB 814 also prevents a person from allowing a BCI it manufactures to be used to bypass the conscious decision-making of an individual unless the person has received specific, written informed consent from the individual. "Specific" in this context means written consent for each and every category of action performed by the BCI. A person receiving written informed consent from an individual shall keep a record of the individual's consent. HB 814 makes clear that consent obtained by using a conscious bypass is not informed consent.

Enforcement: If a person violates HB 814, it would be considered an unfair or deceptive act under Vermont's Consumer Protection Act. Each violation can result in a civil penalty up to $10,000. The Vermont attorney general has the authority to enforce the law and can bring a civil action. Consumers also have a private right of action pursuant to the Vermont Consumer Protection Act.

Effective date: If passed and ultimately signed into law, HB 814 would become effective on July 1, 2026.

7. **Virginia HB 654**

Summary: Virginia HB 654 amends the VCDPA by expanding the definition of "biometric data" to include neural data.

Key definitions: HB 654 updates the definition of "biometric data" to mean "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, facial feature pattern characteristics, neural data, physiological activities, or other unique biological patterns or characteristics that are used to identify a specific individual." HB 654 further specifies that biometric data includes data generated from a physical or digital photograph or a video or audio recording and data stored for healthcare treatment, payment or operations under the Health Insurance Portability and Accountability Act (HIPAA). HB 654 defines "neural data" as "data generated by measurements of the activity of an individual's central or peripheral nervous system that can be processed by or with the assistance of technology."

Application: HB 654 amends the VCDPA, which applies to persons that conduct business in Virginia or produce products or services targeted to residents of Virginia, and that during a calendar year, control or process data of at least 100,000 consumers (i.e., Virginia residents acting in an individual or household context), or control or process personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.

Obligations: HB 654 prohibits consumers, controllers, processors or affiliates, as those terms are defined in the VCDPA, from processing biometric data, including neural data, concerning an individual without obtaining the individual's consent, or in the case of the processing of biometric data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (COPPA).

Enforcement: The Virginia attorney general has exclusive authority to enforce the VCDPA and may seek an injunction to restrain violations of the act, as well as civil penalties of up to $7,500 per violation (following notice of an actual or potential violation by the attorney general to the data controller or data processor and a 30-day cure period).

Effective date: HB 654 is silent as to its effective date.

On February 4, 2026, the Technology and Innovation Subcommittee of the Virginia House of Delegates voted to lay on the table HB 654, effectively halting the bill's advancement for the legislative session.

8. **Vermont HB 791**

The Vermont Legislature introduced HB 791, known as the "Vermont Government Data Practices Act" in January 2026. HB 791 only applies to government entities. Given the focus of this survey on neural data regulations' applicability to commercial businesses, we will not analyze this law in detail.

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
Sam Grogan New York	sgrogan@cooley.com +1 212 479 6344

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.