"You Read My Mind": Neural Data and the New Wave of Biometric Privacy Protections

With recent advances in neurotechnology, a number of states have passed, or are considering, substantial laws regarding a broad spectrum of technologies. These laws impact not only new technologies that can monitor our thoughts, but also older technologies that pose a few new risks.

The neurotechnology subject to these laws encompasses everything from medical electroencephalography (EEG) equipment—with broad uses in measuring electrical activity in the brain to diagnose epilepsy and seizures or investigate sleep disorders, as well as new uses like Neurode's wearable ADHD-monitoring headband—to implantable brain-computer interfaces (BCIs) such as Elon Musk's Neuralink. Some neurotechnology can generate, collect, and alter large swaths of "neural data," defined broadly as information that is derived from and that directly reflects the activities of one's nervous system, including one's central nerves (i.e., the brain and spinal cord) and peripheral nerves. While other personally identifiable information describes people and their activities, some neural data can probe an individual's emotions, mental well-being, and even intentions.

As with many new technologies, efforts to decode neural data can offer countless benefits but can come with significant risks. On the positive side, doctors for years have harnessed patterns in brainwaves to predict seizures, manage depressive disorders, cure sleep issues, and evaluate brain injuries and diseases. New technologies have been, or may be, implemented to take neurotech into new venues. For example, schools may tailor curricula to students' individual learning styles, businesses may target advertisements based upon individuals' needs and desires, law enforcement officers may narrow an investigation or identify particular suspects, and mute individuals may translate their thoughts into speech.

Unfortunately, because of neural data's ability to reveal the fundamental characteristics of one's identity and cognitive processes, the potential for misuse is high. Access to, collection of, and dissemination of neural data without meaningful limitations enables others to surveil, manipulate, exploit, and discriminate against data subjects, even when such data is reportedly anonymized. In the wrong hands, our own thoughts could become a weapon against us.

An increasing number of states and countries have identified the need for robust protection of neural data and proposed or passed related legislation. The changing, uncertain landscape creates a moving target for compliance.

State Legislation

Ten states have drafted legislation explicitly targeting neural data, with four of these bills having passed. These laws are far from uniform, with each defining and treating neural data differently, thus creating a patchwork of compliance obligations for businesses operating in multiple states.

Colorado

Colorado became the first state to pass protections for neural data when Governor Jared Polis signed the Protect Privacy of Biological Data Act (HB24-1058) (Colorado Act) into law.

Effective August 7, 2024, the Colorado Act expands the definition of "sensitive data" under the Colorado Consumer Privacy Act (CPA) to include "biological data," which is "data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or *neural properties*, . . . which data is used or intended to be used . . . for identification purposes." Biological data expressly includes neural data, which is defined as "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."

The Colorado Act's legislative declaration notes that the legislators' primary regulatory objective was protecting individual freedom, especially as it pertains to health, emotions, and cognition. Whether the Colorado Act will regulate uses of neural data beyond use for identification purposes is yet to be determined.

These protections for neural data under the Colorado Act even apply to entities that are not otherwise subject to the CPA. The Colorado Act requires opt-***in*** consent. Entities covered by the Colorado Act must obtain clear, freely given, informed, specific, affirmative, and unambiguous consent from data subjects *before* collecting, processing, or disclosing neural data. The covered entities also must not use dark patterns (any practice that has the effect of limiting individual choice, such as making opting out more difficult than opting in) to obtain these consents and must either refresh consents every 24 months or provide a user-controlled interface for data subjects to manage their opt-in preferences.

California

California followed Colorado's lead by passing an amendment (SB 1223) (CCPA Amendment) to the California Consumer Privacy Act (CCPA) that tackles protections for neural data.

Effective January 1, 2025, the CCPA Amendment redefines "sensitive personal information" to include neural data, defined as "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*." The express exclusion of data that is inferred from nonneural information potentially excludes behavioral and physiological data that can be used to infer one's mental states, but such data may still qualify as "biometric information" under the CCPA and thus be subject to its heightened protections for sensitive personal information.

The CCPA Amendment generally follows the Colorado Act's protections, but with notable differences in impact. First, the CCPA Amendment's protections and rights apply not only to consumers but also to employees. Second, the CCPA Amendment does not require opt-in consent, but merely requires the right to opt ***out*** of processing neural data. Covered entities must provide notice to data subjects at collection, and data subjects have a limited right to opt out of use and disclosure of their neural data if the purpose for such processing is something other than the provision of the good or service that the data subject requested. This opt-out right does not apply to neural data and other sensitive personal information that is collected or processed without the purpose of inferring characteristics about the data subjects.

Connecticut

Connecticut's neural data protections blend the approaches taken in Colorado and California.

Effective July 1, 2025, the Act Concerning Broadband Internet, Gaming, Social Media, Online Services and Consumer Contracts (SB 1295) (Connecticut Act) defines "sensitive data" to encompass nine broad data categories, including neural data. "Neural data," in turn, is defined as "any information that is generated by measuring the activity of an individual's *central* nervous

system." Connecticut's act notably regulates data from the brain and spine but eschews data from the limbs, organs, and skin.

Connecticut's neural data regulations apply to entities that control or process consumers' sensitive and/or neural data, even if the entities do not otherwise meet the general applicability thresholds of the Connecticut Data Privacy Act (CTDPA). As in Colorado, covered entities in Connecticut must obtain clear opt-***in*** consent before using, disclosing, selling, or otherwise processing neural data. Dark patterns are prohibited, and covered entities must disclose relevant information in a privacy notice (including whether the entity will process personal data for the purpose of training large-language artificial intelligence models). Covered entities must also conduct annual data impact assessments.

Montana

Montana extended its existing safeguards for genetic information to neural data when it passed an amendment (SB 163) (GIPA Amendment) to its Genetic Information Privacy Act (GIPA).

Effective October 1, 2025, the GIPA Amendment creates a distinct category of "neurotechnology data," defined as "information that 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." Similar to California's CCPA Amendment, Montana's definition of neurotechnology data expressly excludes "nonneural information, which means information about the downstream physical effects of neural activity, including by (sic) not limited to pupil dilation, motor activity, and breathing rate."

GIPA only governs the data-processing activities of a limited class of "entities," defined as a partnership, corporation, association, or public or private organization of any character that: (1) offers consumer genetic testing products or services directly to consumers; or (2) collects, uses, or analyzes genetic data. Such entities must publish two privacy policies—one high-level overview of the entity's processing activities, and a prominent, publicly available notice that includes complete information about the entity's data collection, consent, use, access, disclosure, transfer, security, retention, and deletion practices.

As in Colorado and Connecticut, covered entities must obtain opt-***in*** consent to collect, use, and disclose neural data. However, the GIPA Amendment also requires these entities to obtain separate, additional express consents for the following activities: (1) transferring or disclosing neural data to a third party (including any employer or entity offering health insurance); (2) using neural data beyond the primary purpose for which it was collected; (3) marketing to consumers based upon neural data; (4) selling neural data; and (5) transferring or storing neural data outside the United States.

Legislation in Progress

Additional states are riding the neural-data-privacy wave, with bills of varying scope and substance pending in their respective chambers.

Illinois drafted an amendment (HB 2984) to its Biometric Information Privacy Act that would expand the definition of "biometric identifier" to include neural data. The bill, in turn, defines "neural data" as information generated by the measurement of activity of an individual's *central or peripheral* nervous system, and *that is not inferred from non-neural information*. The bill requires entities to provide notice to individuals about how such data is collected and stored. Entities must obtain express opt-in consent before collecting, using, storing, or sharing such data.

Massachusetts proposed its Neural Data Privacy Protection Act (HB 103), which defines "neural data" in the same manner as Illinois's amendment but places neural data within the ambit of "sensitive covered data." The bill prohibits covered entities from: (1) collecting or processing neural data unless doing so is strictly necessary to provide a requested good or service; (2) processing neural data for purposes of targeted advertising; and (3) disclosing neural data to third parties without clear consent. The bill also provides consumers with rights to access, correct, delete, and copy their collected neural data.

Minnesota also introduced a standalone bill (SF 1240) that codifies a right to "mental privacy" and "cognitive liberty." The bill prescribes separate neural-data-related compliance obligations for private and governmental entities. Private companies must not use BCIs to bypass conscious decision-making and must provide data subjects with the right to change their decisions regarding the use of neurotechnologies, to protect against unauthorized access to or manipulation of their brain activity, and to protect against unauthorized neurotechnological intervention and alteration of the data subjects' mental functions. Government actors must not collect data transcribed directly from brain activity or use neurotechnologies to interfere with one's free and competent decision-making without informed consent.

Vermont has taken an even more comprehensive approach by introducing three separate bills that target neural data.

The Age-Appropriate Design Code Act (H.210) would prohibit covered entities that develop and provide online services, products, or features that children (i.e., individuals under the age of 13) are reasonably likely to access from using abusive or privacy-invasive design features. The bill provides specific protections for neural data, defined as "information that is collected through biosensors and that could be processed to infer or predict mental states."

The Data Privacy and Online Surveillance Act (H.208) would create comprehensive consumer privacy protections, offering the same protections for neural data as those proposed in the Age-Appropriate Design Code Act.

Lastly, the Act Relating to Neurological Rights (H.366) provides for consumer rights specific to neural data. Such rights include the right to prohibit the collection of neural data from BCIs without prior notice and informed written consent. The bill also prohibits the sharing of neural data with third parties without prior notice and informed written consent.

Federal Efforts

The United States has not yet adopted federal protections for neural data.

Existing laws such as the Health Insurance Portability and Accountability Act of 1996 and its accompanying rules and regulations (collectively, HIPAA) govern neural data only to the extent such data falls within the definition of "protected health information" that is received or created by HIPAA "covered entities" or their "business associates."

However, the United States Senate has identified neural data as a legislative priority, with Senators Charles Schumer, Maria Cantwell, and Ed Markey introducing the Management of Individuals' Neural Data (MIND) Act of 2025 (S. 2925). The bill defines "neural data" as information obtained by measuring the activity of an individual's *central or peripheral* nervous system through the use of technology. If passed, the bill would allocate $10 million to the Federal Trade Commission to spend one year conferring with such stakeholders as the Director of the Office of Science and Technology Policy, the Commissioner of Food and Drugs, and relevant federal agencies to explore whether the existing legal regime adequately addresses neurotechnology or whether additional protections for

neural data are necessary.

International Legislation

Other countries have joined in the push to regulate the processing of neural data.

The European Union's General Data Protection Regulation (GDPR) does not explicitly protect neural data. Neural data may, however, qualify as biometric data, health data, or a "special category" of data, subject to such enhanced protections as the requirements to obtain explicit consent from data subjects, disclose the purposes for which the data is or will be used, and process data for a substantial public interest on a basis proportionate to the aim pursued.

Spain and the United Kingdom published separate reports discussing both the implications of neurotechnology under existing legal frameworks and the potential risks to fairness and accuracy associated with neural data.

Arguably, however, no country has gone as far as Chile. In 2021, Chile became the first country to regulate neural data when the Chilean Senate unanimously approved a bill to amend the country's constitution to include a neural privacy right. Chile recognized the high risk that developers of medical and commercial neurotechnologies could misuse neural data. Chile intended to give one's mind the same status as one's organs, which cannot be bought, sold, or manipulated. The new constitutional right protects data subjects' related rights to mental privacy, free will of thought, equitable access to technologies that increase human capacities, and protection against discrimination. The Chilean Supreme Court has already interpreted the right favorably in a landmark ruling against United States–based neurotechnology company Emotiv in 2023.

Best Practices

As with other laws protecting privacy generally, though drafted with an intent to limit risk, inconsistencies among these legislative developments could limit their usefulness and create undue burdens. Stark differences among these bills as to which entities are covered, how neural data is defined, and what purposes are regulated make taking steps toward compliance with such laws more daunting. Nonetheless, entities should mobilize now to ensure they are prepared for this new frontier of data privacy protections.

First, entities should determine which, if any, of these laws apply to them by identifying whether the entity's goods or services collect, process, or derive neural data of any kind. Remember that in certain states, "neural data" includes data that has been collected for many years. After such determination, companies should map their downstream use, disclosure, and retention practices.

Entities should also implement safeguards from the earliest stages of development of any neural-related technologies and offerings. Entities should monitor their compliance with existing sensitive data privacy regimes, including by creating or revising policies to address when and how neural data is processed. Those policies must be clear, accessible, and correct. Entities should collect and maintain comprehensive records for opt-in and opt-out consents and limit the purposes for which neural data is used.

Questions About Neural Data and Biometric Privacy Protections

These legislative developments demonstrate the growing trend toward strengthening privacy

protections for neural data amid the rise of neurotechnologies and artificial intelligence. Proactive planning and policy updates are critical.

We will continue to monitor developments and any future neural data legislation. If you have any questions about how these laws affect your business, or if you need advice about how to maximize your compliance, please contact the authors or your primary Bass, Berry & Sims attorney.

Resource: Data Privacy Regulations by State

The data privacy regulatory landscape continues to evolve rapidly across jurisdictions. Our privacy & data security attorneys are actively tracking new legislation and regulatory developments nationwide. We will continue to provide ongoing analysis as new regulations emerge. Access our interactive map to learn more about comprehensive state laws and consumer health data privacy requirements.