Division of Legislative Services
ISSUE BRIEF

Neural Data Privacy

By: Grace Kelley, Legislative Research Analyst
February 17, 2025

OVERVIEW

Neurotechnology is defined as "the field of devices and procedures used to access, monitor, investigate, assess, manipulate, or emulate the structure and function of the neural systems of animals or human beings", according to UNESCO's International Bioethics Committee Report from 2021. Neurotechnology is most often associated with medical technological devices that directly record human brain activity or directly influence or modify brain activity to improve quality of life (i.e. cochlear implants, deep brain stimulation, neuro-prosthesis). However, neurotechnology devices have expanded beyond medical and research purposes, appearing in sectors like education, human enhancement, and entertainment. Specifically, direct-to-consumer[1] neurotechnology devices have gained popularity in recent years, ranging from neurogaming[2] and headsets or ear pods, to personal well-being or health devices. Accordingly, investments in neurotech companies have increased by over 600% from 2014 to 2021.

As the access and utilization of neurotechnology surges, the privacy and protection of neural data is a growing world-wide concern. Neural data, also known as brain data, is defined by the Organization for Economic Cooperation and Development as "data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states". Neural data has the potential to reveal intimate personal details about an individual, and if such data is used in combination with artificial intelligence (AI), inferences about an individual can be made solely from neural data collected. With limited regulations, neural data collected is vulnerable to co-optation, unauthorized reuse, and digital surveillance, among other types of unsolicited misuses.

In a study published in April 2024, the NeuroRights Foundation assessed the privacy policy and user agreement documents of 30 companies that provide direct-to-consumer neurotechnology devices. The study found that 29 of the 30 companies have access to consumer neural data and provide no limitations to such access. Additionally, over 60% of the companies' policies do not disclose how consumer neural data is managed and what rights consumers have in relation to it. Most of the companies mentioned in the study are based in countries with already existing data protection laws. However, neural data is not explicitly recognized as personal or sensitive data in these jurisdictions, leaving neurotechnology consumers unprotected.

In 2021, Chile was the first country to introduce a Constitutional amendment protecting the right to mental privacy, integrity, and liberty. Argentina, Brazil, Mexico, and Spain have also introduced legislation to protect neural data privacy. In the United States, there are two states that recognize and

[1] Direct-to-consumer neurotechnology is neurotechnology devices that can be obtained without the involvement of clinicians, researchers, or other third parties.
[2] Neurogaming is a novel form of gaming that involves the use of brain-computer interfaces (BCIs) such as EEG helmets so that users can interact with the game without the use of a traditional controller.

protect neural data legislatively as of 2024: California and Colorado. In 2023, Delaware passed the Personal Data Privacy Act which outlines consumer personal data rights. Under this Act, Delaware residents have the right to know, see, correct, or request deletion of their personal data. However, neural data is not explicitly mentioned as a form of personal data under the Act.

Advantages of Neural Data Privacy Laws

- **Consumer Protection**
  Neural data derives from an individual's central and peripheral nervous system, including brain activity. It can reveal intimate and personal details about a person's cognition, mentality, and unconscious biases. Neural data privacy laws play a role in maintaining mental autonomy and preventing potentially harmful misuse of neural data.

Challenges of Neural Data Privacy Laws

- **Limited Framework on Comprehensive Neural Privacy Protections**
  Very few jurisdictions in the world have introduced or passed measures to protect neural data. There are a multitude of factors to consider when drafting neural data privacy laws:
  - Defining neural data in a way that is neither too broad nor too narrow.
  - Limiting the purpose or intent of legislation to prohibit certain applications or uses of neural data as opposed to legislating neurotechnology devices alone.
  - Balancing data protection requirements and scientific research accessibility, collaboration, and equitability.
- **Rapidly Transforming Technological Landscape**
  The convergence of neurotechnology with AI and existing direct-to-consumer technology is consistently evolving. As neurotechnology devices expand beyond medical and research sectors, it is imperative to monitor how neurotech intertwines with various technology accessories that collect additional types of sensitive data (i.e. biometric, genetic), and the overall implications for consumer protection.

Neural Privacy Laws in the United States

- **Colorado**
  In 2024, Colorado enacted HB 24-1058, expanding the definition of "sensitive data" to cover both biological data and neural data within Colorado's Privacy Act. Under Colorado's statute, neural data 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" and is considered a subset of biological data.
- **California**
  Also in 2024, California enacted SB 1223, amending the definition of "sensitive personal information" in the California Consumer Privacy Act to include a consumer's neural data. The statute defines neural data as "information that is generated by measuring the activity of a consumers central or peripheral

nervous system, and that is not inferred from nonneural information".

- **Minnesota**
  The Minnesota Legislature introduced SF 1110 in 2023, which would have established neurotechnology data privacy rights for consumers. However, this bill failed to leave committee.

Considerations for Delaware Legislators

- **Amending the Delaware Personal Data Privacy Act's Definition of Sensitive Data**
  In 2023, the Delaware Personal Data Privacy Act was signed into law and took effect January 1, 2025. This act aims to protect consumer "sensitive data" by increasing overall transparency of data collection and usage, while expanding consumer rights over their personal data in general. Neural data is not explicitly mentioned under the definition of "sensitive data" in the Delaware Personal Data Privacy Act. With the market for direct-to-consumer neurotechnology devices expanding, the state-level protection of consumer neural data is worth considering, as these devices reach beyond the scope of federal health data protections afforded under the Health Insurance Portability and Accountability Act (HIPAA).

Additional Resources

- Full report on the ethical issues of neurotechnology from the International Bioethics Committee of the United Nations Educational, Scientific, and Cultural Organization (UNESCO).
- A detailed overview of neural data and its potential uses published by the European Data Protection Supervisor in 2024.
- Neuro Technology Toolkit published by the Organization for Economic Coordination and Development (OECD) to support policymakers.
- A list of 30 neurotechnology companies that sell direct-to-consumer neurotechnology devices (pg. 21-29).