INSIGHTS

Technology

U.S. Senators Propose "MIND Act" to Study and Recommend National Standards for Protecting Consumers' Neural Data

Four states include neural data in their consumer data privacy laws, but federal law would go further, requiring federal studies and a framework to protect neural and other related data and permit beneficial use of neurotechnology

By Nancy Libin, Wendy Kearns, Jeremy Ben Merkelson, and Elyse Sparks*

10.15.25

Several weeks ago, U.S. Senators Cantwell (D-WA), Schumer (D-NY), and Markey (D-MA) announced plans to introduce the Management of Individuals' Neural Data Act of 2025 (the "MIND Act" or "Act") which would direct the Federal Trade Commission ("FTC") to study the collection, use, storage, transfer, and other processing of neural data, which "can reveal thoughts, emotions, or decision-making patterns," and certain related data that can reveal cognitive, emotional, or psychological states or neurological conditions. Currently, while there is no comprehensive federal privacy law or federal law covering neural data, a few states have amended their privacy laws to regulate certain aspects of neural data (as discussed below). The proposed Act would not create a new federal regulatory scheme but would instead direct the FTC to conduct a study, issue a report regarding its findings, identify regulatory gaps, and make recommendations to help safeguard consumer neural data and categorize beneficial uses, such as in medical, scientific, and assistive applications.

The neurotechnology at the core of the MIND Act includes consumer wearables and brain-computer interfaces ("BCIs"), but the Act would apply broadly to any "device, system, or procedure that accesses, monitors, records, analyzes, predicts, stimulates, or alters the nervous system of an individual to understand, influence, restore, or anticipate the structure, activity, or function of the nervous system." Devices affected would include smart glasses and watches, clothing with embedded sensors that collect and process biometric information, and headbands that process neural data to aid meditation and sleep. And beyond data obtained directly from both the central nervous system (e.g., the brain and spinal cord) and the peripheral nervous system (i.e., the network of nerves that connects the central nervous system to the rest of the body), the Act directs the FTC to consider "other related data" such as heart rate variability, eye tracking patterns, voice analysis, facial expressions, and sleep patterns captured by consumer wearables and other biosensors.

Companies that are selling, using, and developing technology that processes neural and other related data should follow these developments. This issue

builds on our earlier discussions of neurotechnology advancements and the workplace, technology, and privacy considerations they raise.

What is neural data?

The MIND Act defines neural data to mean "information obtained by measuring the activity of an individual's central or peripheral nervous system through the use of neurotechnology." This data is sensitive because it can reveal our thoughts, feelings, and mental activity, as well as medical conditions that individuals might not want to share. Neural data also allows for inferences of sensitive information, including an individual's susceptibility to addiction or even someone's political beliefs. The Act's sponsors are concerned that neural data could be monetized and used to manipulate, discriminate against, or otherwise undermine consumers' autonomy and civil liberties, and, in the hands of a foreign adversary, to threaten national security. The stated goal of the Act is to ensure strong protections are in place to ensure transparency and accountability, safeguard privacy and security, and prevent discrimination and exploitation so that business can innovate responsibly and consumers can enjoy the benefits of the new products and services that neurotechnology enables.

What would the MIND Act do?

The Act would direct the FTC, in consultation with the Office of Science and Technology Policy ("OSTP"), the Food and Drug Administration ("FDA"), other relevant federal agencies, and a variety of stakeholders—including representatives from private industry—to study the following issues:

- What additional authorities, if any, are needed to regulate neural data and other related data;
- Best practices to protect the privacy and security of such data; and
- How existing laws and regulations govern such data and whether these laws and regulations need to be amended to address any gaps in protection.

Within one year, the FTC would be required to submit a comprehensive report to Congress detailing its findings and recommendations, including the following:

- A regulatory framework to govern neural data and other related data that both fosters innovation and protects against privacy and security risks, including risks of discrimination, profiling, surveillance, manipulation, and misuse;
- Categorization of neural data based on sensitivity, with stricter oversight for high-risk applications;
- Guidance for assessing harms when neural data and other related data is processed by artificial intelligence systems or systems designed to influence behavior or decision making;
- Recommendations regarding the use of such data in particular sectors that may present heightened risk, such as employment, education, healthcare, financial services, and "neuromarketing";
- Whether certain use cases, such as manipulation of behavior or discriminatory profiling, should be prohibited regardless of consent;
- Enhanced cybersecurity protections to address risks in data storage and transfer, including foreign investment and supply chain vulnerabilities; and
- Binding guidance for federal agencies to ensure ethical use of neurotechnology, with transparency and opt-in consent mechanisms.

Although the senators' statement accompanying the Act is focused on preventing harm to consumers, the Act recognizes and directs the FTC to categorize beneficial use cases, "including how such data may serve the public interest, improve the quality of life of the people of the United States, or advance innovation in neurotechnology and neuroscience," which would include advances in assisting paralyzed people move their limbs and use brain-to-text systems for writing, After the report is submitted, OSTP would be

required to develop binding guidance regarding the procurement and operational use by federal agencies of neurotechnology that collects, uses, procures, or otherwise processes neural data or other related data.

Need for a Nationwide Framework

Several states—California, Montana, Colorado, and Connecticut—have recently amended their privacy laws to regulate "neural data"—or "neurotechnology data," in the case of Montana. These states have defined "neural data" differently, however:

- **California, Montana,** and **Colorado** define neural data to include data from both the central nervous system ("CNS") and peripheral nervous system ("PNS"), while **Connecticut** limits its definition to CNS data only.
- **California** excludes algorithmically derived data, such as heart rate variability or sleep scores, while **Colorado** includes such data in its definition.
- **Montana** excludes information derived from the "downstream physical effects of neural activity," such as pupil dilation, motor activity, and breathing rate.

Moreover, these states impose different obligations with respect to such data, making compliance challenging for businesses that operate in this space. For instance, California, Colorado, and Connecticut amended the definitions of "sensitive data" in their privacy laws to include "neural data," but only Colorado and Connecticut require opt-in consent before processing sensitive data, and "neural data" is regulated under Colorado law only when it is used or intended to be used to identify a specific individual. And California merely requires businesses to give consumers the chance to opt out of the processing of their sensitive data if such data is used to infer characteristics about them and is *not* processed for one of several permissible purposes.

By contrast, the MIND Act would direct the FTC to develop a blueprint for a comprehensive nationwide neural data privacy law that could preempt the

state patchwork that is emerging. This would help industries develop neurotechnology more efficiently and streamline the introduction of new products to market.

Concerns About Possible Overbreadth

The MIND Act adopts a very broad definition of neural data that includes information from *both* the CNS, from which data is measured directly through technologies like BCIs or EEGs, and the PNS, which reflects physiological responses, such as heart rate or motor activity, that may only indirectly, at best, suggest mental states. Defining "neural data" to include data from the PNS is somewhat controversial. Those in favor of regulating data from the PNS argue that limiting neural data to measurements obtained directly from the CNS excludes valuable insights into cognitive states that can be inferred from other biometric data. Those who are opposed contend that such data should not be subject to heightened protection because it does not measure brain activity and therefore does not directly reveal thoughts or emotions. Indeed, many categories of non-neural data, like purchase history or engagement metrics, can be used to infer information about someone's motivation, mood, or preferences, and such data is not deemed "sensitive" under privacy laws.

The Act also ties its definition of neural data to data "captured by neurotechnology." Although this limits neural data to information captured through specific tools, the FTC may want to consider revising the definition to accommodate the evolving nature of "neurotechnology." Further, if a future regulatory framework protects "other related data" in addition to neural data, consumer products not explicitly designed to collect "neural data" might be included in a future regulatory effort.

Promoting Responsible Innovation in Neurotechnology

The MIND Act could establish ethical guardrails around what constitutes responsible use of consumer wearables that track neural data. This could foster consumer trust and increase the innovation of, and demand for, such products.

In the medical field, for example, neurotechnology is driving groundbreaking

advancements by using BCIs to enable paralyzed individuals to control devices like external limbs and computers. For instance, in 2024, Neuralink successfully implanted a chip in a patient's brain, allowing the patient to control a computer cursor with his mind. Neuralink is now positioned to begin a new clinical trial in October for a brain implant that can read speech and create text directly from the brain. Technology like this would allow consumers to directly speak to large language models and other artificial intelligence ("AI") systems at the speed of thought, and potentially hear a response from the AI model through their earbuds.

Many other companies also are developing neurotechnology in the consumer space. Products include Meta's Neural Band, which allows individuals to control their smart glasses with minor movements from their wrists and hands. In addition, Tobii, a Swedish company, sells eye-tracking glasses designed to enhance safety measures and quality inspections in factories, analyze the expertise and habits of skilled employees to support training, and improve pilot performance and safety.

At the same time, the prospect that employers might deploy non-invasive, wearable neurotechnology to monitor employees in the workplace, assess their productivity and fatigue levels, identify performance lapses, and other so-called "neuroergonomic" uses, raises real ethical quandaries about where to draw the limits around corporate surveillance in this new age. Scholar Nita Farahany, among others, has advocated for strong federal protections at least in part because of the potential for workers to be disciplined based not on what they do or say but rather based on how they think or feel.

We expect that the FTC's Report could encourage beneficial medical and other consumer uses while identifying reasonable boundaries to protect consumers and workers.

Businesses' Opportunity to Shape Legislation

The MIND Act gives businesses an opportunity to shape regulatory frameworks governing neural and other related data and neurotechnology. As noted above,

the Act directs the FTC to consult with private-sector stakeholders, academia, and consumer advocacy groups.

By participating in this process, businesses can educate lawmakers about the many beneficial uses of neural data and neurotechnology, as well as provide insights and best practices regarding the handling of such data. Indeed, by showing the FTC that they recognize and have addressed the privacy, employment and security concerns associated with the processing of neural data and other related data, businesses can potentially stave off new legislation —or at least influence the development of future legislation to align with current practices. And because as part of its report, the FTC would be required to research potential incentive structures and market advantages for companies that prioritize consumer protection, privacy, and ethical innovation, businesses could position themselves to benefit from tax credits, financial support, procurement preferences, or expedited approvals. Finally, businesses should take note that the MIND Act would direct OSTP to craft binding guidance for procurement and operational use of neurotechnology by federal agencies. Although these rules would apply directly to federal contracts and contractors, they could indirectly influence private industry, as businesses align their policies to remain eligible for government contracts.

Conclusion

If you want to learn more about the MIND Act, its advancement in Congress, what consumer wearables innovators are doing to establish private industry rules, or anything else neurotech related.... you read our mind! Please contact the DWT team closely tracking this new and rapidly expanding area of the law and our lives.

** Elyse Sparks is a law clerk at Davis Wright Tremaine.*

Related Insights

10.02.25
INSIGHTS

CISA 2015 Has Sunset. Now What?

09.17.25
INSIGHTS

CISA Delays Cyber Incident Reporting Rules Until May 2026

09.12.25
INSIGHTS

Department of Defense Issues Final Rule to Implement Cybersecurity Maturity Model Certification (CMMC) Program