Mind Your Mind: What the MIND Act Means for the Future of Privacy

September 28, 2025 - Three senators - Chuck Schumer of New York, Maria Cantwell of Washington, and Ed Markey of Massachusetts - recently introduced the MIND Act, short for the Management of Individualsâ€™ Neural Data Act of 2025. The bill directs the Federal Trade Commission to study how brain wave and other neural data should be safeguarded as consumer devices capable of measuring and interpreting the nervous system become more common. Supporters say it is important to act now because companies are already experimenting with headsets, implants, and other technologies that may collect deeply personal information about peopleâ€™s thoughts, emotions, and decision-making patterns. Unlike medical records covered by HIPAA, most of this data is collected outside health care and falls into a gray area where few protections exist.

The bill is a first step rather than a strict rule. It orders reports and recommendations but does not yet create penalties or enforceable rights. That has led some privacy experts to call it a recognition of the problem but not a full solution. At the state level, laws in Colorado, California, and Montana already recognize neural data as sensitive and require consent before collection. Abroad, Chile amended its constitution to include a right to neuroprotection, and European law already includes protections for mental integrity.
The larger issue is that we still donâ€™t know what long-term risks come with collecting neural data. On its own, a few minutes of brain wave signals may seem harmless. But combined over time and analyzed with advanced algorithms, this information could expose how a person is feeling, whether they are paying attention, or even signs of mental health conditions. Such insights could be used to target advertising at moments of weakness, push high-risk financial products, or screen people for insurance or employment. Once neural data is exposed, it cannot be changed like a password.

If that sounds far-fetched, history with biometric data shows how quickly sensitive information can be misused. In 2024, Meta agreed to pay $1.4 billion to settle a lawsuit in Texas over its use of facial recognition technology without proper consent (Reuters, July 30, 2024). Clearview AI, a company that scraped billions of photos to build a facial recognition database, has been fined in Europe and faces restrictions in the United States for collecting faces without permission. In Illinois, businesses have faced class actions under the stateâ€™s Biometric Information Privacy Act for collecting fingerprints or facial scans without consent, including cases involving simple time-clock systems for workers. These examples highlight the risks of allowing private companies to collect sensitive biological identifiers first and worry about rules later. Neural data may be even more intimate and more difficult to protect once in circulation.

The MIND Act does not resolve all of these challenges, but it signals that Congress is beginning to grapple with them. As technology develops, guardrails will be needed to make sure innovation serves people rather than exploits them. For consumers, the lesson is to be aware that new gadgets promising convenience or even health benefits may also be quietly collecting information no one has ever had access to before. We do not yet know how valuable or dangerous that information might become, which is why the push to study and eventually regulate it matters now.

by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS