Cybersecurity Law Report cslawreport.com

Feb. 11, 2026

Biometrics

When Thoughts Go Digital: Securing the Rise of Neurotechnology

By Kristen Mathews and Nathaniel Kim, *Cooley*

The world is at the threshold of a revolution where the boundary between biology and silicon is beginning to blur. This field, known as neurotechnology, is anchored by brain-computer interfaces (BCIs), which are extraordinary tools that create a direct bridge between the human brain and external computing devices. By capturing neural signals and translating them into machine-interpretable signals, BCIs allow users to move cursors or robotic limbs through thought alone, bypassing the need for traditional movement or speech.

As with all cutting-edge technologies, the expansion of individuals' capability to read and effectuate neural signals is a double-edged sword. While it opens the door to life-changing medical breakthroughs, it also introduces potential information security risks that are expected in any context where data is collected, transferred or stored. Indeed, as neurotechnology transitions from high-tech labs into humans' daily lives, it brings with it a "neurosecurity" challenge: the need to protect people's most intimate data – their thoughts and neurological patterns. The good news is that industry leaders are moving just as fast as the technology itself, applying lessons learned from earlier fields of connected devices, and proactively baking security principles into the DNA of these devices to safeguard our digital future.

This article examines the benefits of BCIs, theoretical security vulnerabilities, relevant state laws that protect neural information and cybersecurity measures the industry is taking to combat cyber threats.

See this two-part series on the sale of 23andMe's genetic data: "Implications of the Motions for a Privacy Ombudsman and State Laws" (Apr. 16, 2025), and "Lessons for Companies Around Sensitive Data" (Apr. 23, 2025).

Benefits of Brain-Computer Interfaces

BCIs, and neurotechnology at large, collectively present an exciting frontier of opportunity not only for medicine, but also for a wide variety of industries such as education, entertainment and communication. The therapeutic benefits of BCIs are already proving transformative, particularly for individuals with severe physical limitations. For patients with "locked-in" syndrome or Amyotrophic Lateral Sclerosis (ALS), BCIs offer a vital bridge back to the world. Individuals who have lost the ability to speak or move have used implants to translate their neural intentions into text, allowing them to communicate with others.

Beyond medical applications, BCIs could be used in education to enhance neuroadaptive learning, where systems monitor a student's focus or mental fatigue in real time and adjust the difficulty or pace of a lesson accordingly to prevent cognitive overload. One could use this kind of neurofeedback to inform and facilitate musical training, for example. In the entertainment sector, BCIs are enabling a new era of "passive" gaming and virtual reality, where the digital environment can react to a user's emotional state or visual attention, allowing for hands-free menu navigation and immersive storytelling that shifts based on the player's neural signals.

Possible Security Vulnerabilities

Opening the door to BCIs' life-changing benefits also means reckoning with neurosecurity risks because the use of BCIs necessarily involves collecting and processing information from the brain. Indeed, BCIs share key characteristics with IoT devices – both remain constantly active and depend on continuous network connections. This connectivity brings benefits but simultaneously opens the door to cyber threats. The specific cyber risks of BCIs vary based on their physical architecture and how they acquire neural signals. This article divides the universe of BCIs into implanted and non-implanted (wearable) BCIs, and further sub-divides implanted BCIs into wired and wireless implanted BCIs.

Wired Implanted BCIs

Wired implanted BCIs, which have been around since the 1970s, are surgically implanted into the brain and physically wired to external hardware when they need to transfer data or receive a software update. This is a format typically chosen for high-stakes medical applications because it provides the highest possible signal fidelity. Many users with this type of implanted BCI "unplug" from the external receiver when a connection is not needed and live a relatively normal life.

On the one hand, the wired connection allows the BCI to be free of the various vulnerabilities that are present with a wireless connection. That is, an attacker would have a hard time gaining access to the BCI device's data without a physical connection. But wired implanted BCIs are not completely immune to vulnerabilities. These BCIs still rely on continuous software updates for improved functionality, which means that issues with any of the updates – intentional or inadvertent – can pose a security risk.

Furthermore, data that is transferred from the implanted component to the external component for processing should be encrypted to mitigate against the risk of unauthorized access or unintentional disclosure. And, in some circumstances, the physical connection itself can be a vulnerability; the long leads and high-gain amplifiers required to record micro-volt signals can act as unintentional antennas for radio-frequency (RF) interference. BCI developers are on alert for these potential vulnerabilities and can implement mitigative measures against such exploits.

Wireless Implanted BCIs

Wireless implanted BCIs offer a distinct advantage compared to their wired counterparts because they remove the need for a physical connection through the scalp. These devices typically rely on the Bluetooth protocol for data transmission. This wireless convenience introduces an airborne attack surface, making the implant susceptible to Bluetooth vulnerabilities.

Examples of possible attacks historically seen in other Bluetooth-connected devices include Bluebugging and Bluesnarfing, which allow hackers to gain unauthorized access and intercept communications. More sophisticated threats include the BlueBorne vector, which can compromise a device without it being in discoverable mode, or the Key Negotiation of Bluetooth attack, where the bad actor forces the device to use a weak encryption key to decrypt or manipulate the data being transmitted between the device and the external device. If deployed against a BCI device, this could result in inaccurate data or commands being sent to the device, potentially causing the user's neural activity to be misinterpreted. Because Bluetooth vulnerabilities are relatively well-documented and familiar to security professionals, BCI makers are on alert and can take steps to harden security in their products.

Wearable BCIs

Wearable BCIs, such as non-invasive EEG headsets used for gaming or focus training, are the most accessible format for the general public, requiring no surgery and offering relatively easy integration with consumer electronics. These devices include headbands, earbuds, helmets and other wearables, and are less regulated than medical-grade implants.

Laboratory studies have shown that wearable consumer BCI devices can be targeted with RF interference to read and alter the data transmitted between the headset reading the neural signals and the receiver. For example, one lab study demonstrated that an attacker can present a user with specific visual stimuli and record the involuntary brain response to extract sensitive information, such as bank PINs or home addresses without the user's knowledge. Researchers were also able to remotely inject false brain-waves into the BCI devices with amplitude-modulated RF signals, crashing a drone controlled by a headset, tampering with a neuro-feedback meditation interface and forcing a neural signal-to-text translator to input "I HATE MIT" instead of the user's intended message, "I LOVE MIT." As studies report each of these attack vectors, the BCI developer community continues to monitor closely to implement mitigation measures.

See this three-part series on the metaverse IRL: Tackling Privacy Amid the Rampant Hype and Burst of Deals" (Sep. 21, 2022), Grappling With Biometric Data and Privacy Notices in VR Headsets" (Oct. 5, 2022), and "Are Companies Overlooking the Privacy Risks of NFTs and Crypto Wallets?" (Oct. 12, 2022).

U.S. State Privacy Laws That Protect Neural Data

In response to emerging concerns around BCIs, several states have taken aggressive action to amend their existing consumer privacy laws to include neural data.

Colorado

Colorado led the pack in April 2024, by passing HB 24-1058, which amended the Colorado Privacy Act (CPA) to include "biological data" and "neural data" within the definition of "sensitive data." The amended law mandates that any entity collecting such information must first provide clear notice and obtain affirmative consent from the consumer. It also requires companies to conduct data protection assessments for any processing of neural data, as well as to take reasonable measures to secure such data by implementing appropriate technical and organizational measures to secure neural data from unauthorized access. The Colorado legislation went into effect in mid-2024, making it the first comprehensive framework for neural data protection in the nation.

See "Colorado Controllers: The Final (Rules') Frontier" (May 31, 2023).

California

A few months after the CPA's amendment, in September 2024, California mirrored Colorado's protections, passing its own Brain Privacy Act (BPA), explicitly including "neural data" under the definition of sensitive personal information in the CCPA. As a result, companies handling neural data must, among some other requirements similar to the Colorado law, implement robust security safeguards for neural data, affording it the same level of protection as health, banking and biometric records. The BPA became effective on January 1, 2025, establishing a new standard for neurotechnology compliance in the state.

Connecticut

In June 2025, following Colorado and California, Connecticut passed SB 1295 to amend its data privacy law to clarify that "sensitive data" includes "neural data." By doing so, Connecticut also imposed affirmative consent and data protection assessment requirements for entities that handle neural data. The law requires that businesses establish and implement data security practices that are appropriate to the nature of the data. This means that, as a type of "sensitive data," neural data must be protected with a heightened level of security under Connecticut's framework.

See this two-part series on revised privacy laws in Connecticut and Oregon: "Broader Scope and Enhanced Consumer Protections" (Jul. 23, 2025), and "Impact Assessments, Minors and More" (Jul. 30, 2025).

Montana

Montana's SB 163, which amends the state's Genetic Information Privacy Act (GIPA), applies to a broader category called "neurotechnology data," which includes neural data. Among other data protection requirements, the law directs covered entities to establish and maintain a comprehensive security program to protect a consumer's neurotechnology data against unauthorized access, use or disclosure. The amendments to GIPA became effective on October 1, 2025.

See "Saddling Up for Montana's Broad Privacy Law Update" (Jun. 4, 2025).

Industry Cybersecurity Efforts

Industry leaders are increasingly adopting neurosecurity principles to harden their products against cyber threats.

Security by Design

"Security by design" is critical for neurotechnology. It offers a rare opportunity to embed robust protections into the fundamental architecture of BCIs before they achieve mass-market adoption. By integrating encryption, authentication and tamper-resistant protocols during the initial engineering phase, the industry can preemptively close or narrow the biological attack surface that often plagued retrospective security efforts in the now-mature consumer IoT sector. These security-hardening measures have the added benefit of getting ahead of long-term compliance costs, as global regulators contemplate raising regulatory scrutiny of BCI devices in the market. For example, the Organisation for Economic Co-operation and Development released a neurotechnology toolkit last year recommending that policymakers encourage developers to adopt "safety by design" principles and consider cybersecurity risks in their safety assessments. Ultimately, taking a proactive stance toward neurosecurity ensures that cognitive liberty and physical safety are not treated as peripheral features, but as foundational requirements for the future of human-computer interaction.

Coordinated Cybersecurity Measures

Managing neurosecurity risks requires developers to take multiple coordinated measures, including:

- deploying advanced encryption;
- establishing robust authentication processes;
- maintaining regular system updates; and
- providing thorough user training.

Other measures BCI developers can take include providing timely software updates with integrity checks prior to delivery to the BCI device to verify that the update has not been modified before installation. Manufacturers should clearly communicate to users about support windows for each update and implement technical controls for robust user authentication.

Specific defensive strategies developers can employ include the use of "out-of-band" pairing methods to prevent man-in-the-middle attacks and the application of strong encryption for all data moving between the implanted device and its external processing unit. Furthermore, for wireless-enabled devices, industry leaders can prioritize prompt patching of firmware to address known airborne vulnerabilities. By integrating these proactive security measures, the private sector is working to ensure the long-term integrity of BCI systems and maintain the trust of patients and consumers alike.

The Road Ahead

The integration of BCIs into daily life offers a future of restored mobility and enhanced communication, but it also necessitates a new era of cybersecurity. By addressing vulnerabilities at the physical, network and software layers, stakeholders can ensure that the benefits of BCIs are realized while mitigating the known cyber risks.

Neurotechnology cybersecurity researchers are already actively identifying emerging vulnerabilities and proposing mitigation strategies, and industry stakeholders are closely monitoring these findings to guide secure development. As neurotechnology continues to advance, the ongoing collaboration between developers, policymakers and security experts will be crucial for navigating this exciting and dynamic frontier.

Kristen Mathews is a partner at Cooley, working at the forefront of complex privacy and cybersecurity issues. She advises clients on compliance with data privacy laws at the state, federal and international levels. Her long-standing work with innovative technology companies and her early focus on the legal implications of neurotechnology led her to spearhead the development of Cooley's neural privacy resource hub, a first-of-its-kind guide designed to help businesses and researchers navigate the emerging legal landscape surrounding wearable neurotech devices, brain-computer interfaces and mental privacy.

Nathaniel Kim is an associate in Cooley's cyber/data/privacy group. Drawing on his academic and public sector experience in technology law and policy, including his role in the privacy branch of the Office of Information and Regulatory Affairs, he focuses his practice on the intersection of data privacy and emerging technologies. Kim advises innovative companies on compliance with U.S. and international privacy regulations, and represents clients in high-stakes disputes involving privacy and cybersecurity issues.