TO USE YOUR BRAIN, FIRST ACCEPT THE TERMS AND CONDITIONS: LEGAL PROTECTIONS FOR COMMERCIAL BRAIN-COMPUTER INTERFACES

MATHEW YAEGER*

Recent advancements in brain-computer interface (BCI) technology have created significant privacy and autonomy concerns as commercial applications emerge. While Colorado and California have enacted legislation recognizing neural data as sensitive personal information, current legal frameworks remain inadequate to address the unique challenges posed by BCI technology, particularly those concerning mental manipulation and consciousness bypass. This Note examines Minnesota's proposed neural privacy legislation, S.F. 1240, as a model for holistic BCI regulation, analyzing how it addresses concepts such as psychological continuity and mental autonomy. While Minnesota's framework creates important protections against neural influence and data collection, it still faces significant implementation challenges regarding technical standards, consent mechanisms, and enforcement procedures. More fundamentally, the framework faces potential constitutional barriers around First Amendment protections and federal preemption. These challenges suggest that effective neural protections may require solutions beyond traditional state legislation, potentially including federal regulation, industry standards, and international cooperation. As BCI technology advances, establishing comprehensive legal protections for mental privacy and cognitive liberty becomes increasingly urgent, even as perfect solutions remain elusive.

* J.D. Candidate, University of Colorado Law School, Class of 2026. I am grateful to my parents, Robin and Eric Yaeger, for early proofreading and for helping me understand neurological and medical privacy concepts. I am also grateful to Professor Blake Reid for discussions that pushed me to think more critically in developing this work. Finally, thank you to the editors of Volume 24 of the Colorado Technology Law Journal for their thoughtful editing and extensive feedback. All views and errors are my own.

INTRODUCTION

In *1984*, George Orwell cautioned that "[n]othing [is] your own except the few cubic centimeters inside your skull."[1] In that world, the mind remained beyond the reach of surveillance, but the fear of "thoughtcrime"—the crime of merely thinking forbidden ideas—was enough to ensure people's obedience.[2] In Dan Erickson's *Severance*, workers are implanted with a chip that splits their consciousness in two, leaving each half entirely unaware of the

1. George Orwell, NINETEEN EIGHTY-FOUR, at 23 (New Am. Libr. 1952).
2. *Id.* at 17.

other's thoughts and experiences.[3] These dystopian visions of mental invasion and cognitive manipulation—once safely confined to science fiction—are edging ever closer to reality.

Brain-computer interface (BCI) technology, which enables direct communication between the brain and external devices by measuring neural signals, represents the source of these emerging concerns.[4] Significant milestones have already been achieved in the commercial development of these technologies. In 2020, Synchron received Food and Drug Administration (FDA) Breakthrough Device designation for its endovascular BCI system, which allows paralyzed patients to control digital devices through thought.[5] More recently, in January 2024, Elon Musk's Neuralink began its first human trial of an implantable BCI.[6]

The advancement of BCI technology raises unprecedented concerns for privacy and autonomy, especially as commercial applications begin to emerge. Research has demonstrated that BCIs can interpret mental states, recognize emotional responses,[7] and even reconstruct visual imagery directly from brain activity.[8] Studies using advanced machine-learning algorithms have achieved increasingly accurate reconstruction of mental images, suggesting that future capabilities could extend to accessing dreams, memories, and internal visualizations.[9] More concerning are developments in brain stimulation and neural augmentation. Non-invasive brain stimulation technologies have been used to modify fear memories[10] and influence decision-making processes,[11]

3. SEVERANCE: *Good News About Hell* (Apple TV+, aired Feb. 18, 2022), https://tv.apple.com/us/episode/good-news-about-hell [https://perma.cc/N8A2-NPYH].

4. Aleksandra Kawala-Sterniuk et al., *Summary of Over Fifty Years with Brain-Computer Interfaces*, 11 BRAIN SCI. 43, Jan. 3, 2021, at 1, 2–3.

5. Press Release, Synchron, Synchron Announces First Human U.S. Brain-Computer Interface Implant (July 19, 2022, 8:00 AM EST), https://www.businesswire.com/news/home/20220719005248/en/Synchron-Announces-First-Human-U.S.-Brain-Computer-Interface-Implant [https://perma.cc/3JST-H58W] [hereinafter Synchron First U.S. BCI Implant].

6. Alex Hern, *Elon Musk says neuralink has implanted its first brain chip in human*, THE GUARDIAN (Jan. 30, 2024, 7:18 EST), https://www.theguardian.com/technology/2024/jan/29/elon-musk-neuralink-first-human-brain-chip-implant [https://perma.cc/8CSS-DZY9].

7. Alisha Arora, *Brain Computer Interfaces for mental health care*, MEDIUM (Dec. 23, 2021), https://medium.com/@alishaarora56/brain-computer-interfaces-for-mental-health-care-9c7629c048c1 [https://perma.cc/FGU4-5Z5P].

8. Kendrick N. Kay et al., *Identifying Natural Images from Human Brain Activity*, 452 NATURE 352, 352–55 (2008).

9. Naoko Koide-Majima et al., *Mental Image Reconstruction from Human Brain Activity*, 170 NEURAL NETWORKS 349, 361 (2023).

10. Sara Borgomaneri et al., *Memories are not Written in Stone*, 127 NEUROSCIENCE & BEHAVIORAL REV. 334, 336 (2021).

11. *See* Tad T. Brunyé, *Non-invasive Brain Stimulation Effects on the Perceptual and Cognitive Processes Underlying Decision-Making: A Mini Review*, 5 J. COGNITIVE ENHANCEMENT 233, 233 (2021).

while other studies have successfully predicted decisions seconds before individuals become consciously aware of their choices.[12]

The privacy implications of neural technology have already prompted legislative action in multiple states. In 2024, Colorado and California became the first to enact laws explicitly protecting neural data privacy.[13] Several other states followed in 2025, introducing legislation with similar aims.[14] Despite this progress, existing federal and state privacy frameworks remain ill-equipped to address the unique challenges posed by BCI technology. While the Health Insurance Portability and Accountability Act (HIPAA) protects medical information[15] and state privacy laws govern personal data collection,[16] neither adequately addresses the distinct nature of neural data nor the potential for mental augmentation through BCI technology.[17]

Although the amendments to the Colorado Privacy Act (CPA) and the California Consumer Privacy Act (CCPA) are groundbreaking in explicitly recognizing neural data as sensitive personal information, they continue to operate within traditional commercial data collection and consent frameworks.[18] By treating neural data like any other form of sensitive personal information, these laws fail to account for its capacity to reveal thoughts or modify consciousness. Emerging research into memory modification and conscious decision-making modulation further

12. Roger Koenig-Robert & Joel Pearson, *Decoding the Contents and Strength of Imagery Before Volitional Engagement*, 9 SCI. REPS., Mar. 5, 2019, at 1, 7.

13. *See* Perla Khattar, *Neural Data and Consumer Privacy: California's New Frontier in Data Protection and Neurorights*, Tech Policy Press (Nov. 19, 2024), https://www.techpolicy.press/neural-data-and-consumer-privacy-californias-new-frontier-in-data-protection-and-neurorights [https://perma.cc/9N59-4BAC]; H.B. 24-1058, 74th Gen. Assemb., Reg. Sess. (Colo. 2024) (enacted); S.B. 1223, 2023-2024 Leg., Reg. Sess. (Cal. 2024) (enacted).

14. *See* Morrison & Foerster LLP, *More States Propose Privacy Laws Safeguarding Neural Data,* MoFo Privacy Blog (Mar. 17, 2025), https://www.mofo.com/resources/insights/250317-more-states-propose-privacy-laws-safeguarding-neural-data [https://perma.cc/7CXT-2DF3]. Two of these bills—Montana S.B. 163 and Connecticut S.B. 1295—have been enacted, largely mirroring the structure and scope of existing Colorado and California statutes. *See also* S.B. 163, 69th Leg., Reg. Sess. (Mont. 2025); *see also* S.B. 1295, Gen. Assemb., Jan. Sess. (Conn. 2025).

15. HHS, HIPAA Administrative Simplification (Mar. 2013), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf [https://perma.cc/8SN9-NM7G].

16. *See* Müge Fazioglu, US STATE COMPREHENSIVE PRIVACY LAWS REPORT 2-3 (Int'l Assn. Priv. Pros., 2024), https://iapp.org/resources/article/us-state-privacy-laws-overview/ [https://perma.cc/CVH5-ZK3H].

17. *See* Vera Tesink et al., *Right to Mental Integrity and Neurotechnologies: Implications of the Extended Mind Thesis*, 50 J. MED. ETHICS 656, 657 (2024).

18. *See* H.B. 24-1058, 74th Gen. Assemb., Reg. Sess. (Colo. 2024) (enacted); *see also* S.B. 1223, 2023-2024 Leg., Reg. Sess. (Cal. 2024) (enacted).

exposes challenges that extend beyond data privacy concepts.[19] This underscores the need for a new legal framework that recognizes and protects psychological continuity and mental self-determination as fundamental rights.[20]

This Note argues that enacting legislation that more effectively protects neural data privacy and autonomy is necessary before commercial BCI technology becomes widely available. Drawing on Minnesota's proposed neural privacy and autonomy legislation,[21] this Note proposes a regulatory model that balances continuing technological innovation with the need to maintain fundamental privacy rights while addressing the unique challenges posed by emerging BCI technology.

Part I examines the history and ongoing development of BCI technology. Part II analyzes the limitations of current privacy frameworks in their ability to protect neural data, including an examination of Colorado and California's recent legislation. Part III evaluates Minnesota's proposed legislation—centered on concepts such as "consciousness bypass" and "psychological continuity"—and how these provisions provide a more holistic framework for ensuring neural privacy and autonomy. Part IV proposes modifications to strengthen Minnesota's framework and improve its viability. Finally, Part V analyzes the technical, constitutional, and practical challenges that may hinder the effective implementation of neural privacy and autonomy protection frameworks.

I. BRAIN-COMPUTER INTERFACE TECHNOLOGY

The conceptual groundwork for the BCI originated with the publication of Norbert Wiener's book *Cybernetics: or Control and Communication in the Animal and the Machine* in 1948.[22] In this work, Wiener proposed the possibility of direct communication between biological and mechanical systems, particularly focusing on the potential application to prosthetics.[23] He introduced the idea that both the brain and computers function as "logical machines" that process information similarly.[24] While he never used the term

19. *See* Jared Genser et al., INTERNATIONAL HUMAN RIGHTS PROTECTION GAPS IN THE AGE OF NEUROTECHNOLOGY 50 (2022) (discussing how neurotechnologies capable of altering mental processes challenge existing human rights frameworks and require new legal protections).

20. *See id*.

21. Minn. S.F. 1240, 94th Leg., Reg. Sess. (2025) (reintroduced following S.F. 1110, which was introduced in the 2023–2024 legislative session but did not advance).

22. NORBERT WIENER, CYBERNETICS: OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (1948).

23. *Id.* at 139–43.

24. *Id.* at 124.

"brain-computer interface," Wiener's conceptualization established the core ideas that would guide the subsequent decades of research into neural interfaces and brain-machine communication.

The transition from theoretical exploration of BCIs to practical experimentation began with Jacques Vidal's 1973 paper *Toward Direct Brain-Computer Communication*, in which he coined the term "brain-computer interface."[25] Vidal's subsequent experiments with BCIs established the feasibility of using neural signals to enable basic computer control.[26] In one such experiment, he had subjects use their thoughts to guide a cursor through a digital maze.[27]

BCI research following Vidal's experiments has proceeded with two main technological approaches. Non-invasive BCIs that measure brain activity using electroencephalography (EEG) sensors placed on the scalp[28] emerged in the 1970s and offer practical accessibility by avoiding the need for surgical intervention, lowering ethical, clinical, and cost barriers.[29] In the 1990s, researchers began developing invasive BCIs, which rely on electrodes implanted into the brain and enable greater precision in measuring brain activity.[30] This period marked a transition from BCIs existing as an experimental concept to being used as practical tools—with initial uses centered in healthcare.

BCI development experienced a dramatic acceleration in the early 2000s with the emergence of more advanced neural recording technologies and signal processing methods.[31] This period saw the first successful human trials of BCIs designed to assist with communication and motor control, firmly establishing BCIs as viable medical devices.[32] Concurrent advances in neuroscience and computing, particularly in the understanding of neural signal

25. Jacques J. Vidal, *Toward Direct Brain-Computer Communication*, 2 ANN. REV. BIOPHYSICS & BIOENGINEERING 157, 157–58 (1973), https://doi.org/10.1146/annurev.bb.02.060173.001105 [https://perma.cc/ULY7-S3SQ].

26. *See* Jacques J. Vidal, *Real-Time Detection of Brain Events in EEG*, 65 PROCEEDINGS OF THE IEEE 633, 640 (1977).

27. *Id.* at 637–38.

28. *Electroencephalogram (EEG),* MAYO CLINIC, https://www.mayoclinic.org/tests-procedures/eeg/about/pac-20393875 [https://perma.cc/JX2A-QFKY].

29. Xiaotong Gu et al., *EEG-Based Brain-Computer Interfaces (BCIs): A Survey of Recent Studies on Signal Sensing Technologies and Computational Intelligence Approaches and Their Applications*, 18 IEEE/ACM TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS, Sept.-Oct. 2021, at 1645, 1645–47, https://doi.org/10.1109/TCBB.2021.3052811 [https://perma.cc/7XQE-YWSJ].

30. *See* Kawala-Sterniuk et al., *supra* note 4, at 7–8.

31. *Id.* at 7.

32. *Id.* at 7–10.

processing and machine-learning, enabled increasingly sophisticated interpretations of brain activity.[33]

A significant shift has occurred in this decade, with work on BCIs moving from primarily academic and medical research settings into more substantial commercial applications.[34] Startups and major technology companies have begun investing heavily in BCI development, signaling a coming introduction to the consumer market.[35] This commercialization period has coincided with further advances in neural recording technology and artificial intelligence, enabling capabilities previously confined to theoretical discussions.[36] Current BCI applications span a wide range—from medical devices restoring motor function to experimental systems capable of predicting and changing decisions and thoughts—with each application presenting unique capabilities and risks that require careful consideration.[37]

A. Motor Control and Communication

The most well-established applications of BCI technology focus on restoring motor function and communication ability in individuals with severe disabilities,[38] illustrating both the current real-world capabilities and limitations of BCI technology. Advances BCIs' capabilities for motor control and communication demonstrate the increasingly sophisticated interaction between the brain and digital systems. Research indicates that current BCIs can decode complex movement intentions with sufficient precision to enable fine motor control.[39] BCIs can also accurately interpret speech information—even in patients with severe neurodegenerative disorders—allowing for verbal

33. *See* Xue Fan & Henry Markham, *A Brief History of Simulation Neuroscience*, 13 FRONTIERS IN NEUROINFORMATICS, May 7, 2019, at 1, 8–9.

34. *See* Baraka Maiseli et al., *Brain-Computer Interface: Trend, Challenges, and Threats*, 10 BRAIN INFORMATICS, 2023, at 1, 11.

35. *See* Yasmin Khorram, *Inside a $400 Billion bet on the brain-computer interface revolution*, YAHOO FINANCE (Nov. 18, 2024), https://finance.yahoo.com/news/inside-a-400-billion-bet-on-the-brain-computer-interface-revolution-150057794.html?guccounter=1 [https://perma.cc/2WMH-2UTM].

36. *See* Rafael Yuste et al., *Four Ethical Priorities for Neurotechnologies and AI*, 551 NATURE, Nov. 9, 2017, at 159, 159–61.

37. *See* Simanto Saha et al., *Progress in Brain Computer Interface: Challenges and Opportunities*, 15 FRONTIERS IN SYSTEMS NEUROSCIENCE, Feb. 25, 2021, at 1.

38. *See* Wireko Andrew Awuah et al., *Bridging Minds and Machines: The Recent Advances of Brain-Computer Interfaces in Neurological and Neurosurgical Applications*, 189 WORLD NEUROSURGERY, Sept. 2024, at 138, 138.

39. *See* Ksenia Volkova et al., *Decoding Movement from Electrocorticographic Activity*, 13 FRONTIERS IN NEUROINFORMATICS, 2019, at 1, 3 (discussing advances in movement decoding accuracy).

communication.[40] More recent BCIs have improved speech capabilities, achieving real-time brain-to-speech communication.[41] This precision stems from an improved understanding of how the brain encodes movement and speech information, combined with machine-learning models that can interpret these neural patterns in real time.[42] The ability to accurately decode and transmit neural signals represents a fundamental shift in human-computer interaction—from requiring external input devices to allowing direct control from the brain.[43]

Synchron's Stentrode BCI exemplifies the growing accessibility of invasive BCIs as the first implantable system to receive FDA approval.[44] Unlike other invasive BCIs, which require surgical implantation into the main brain structure,[45] the Stentrode is implanted via blood vessels around the brain—eliminating the need for intensive surgery.[46] While its development is still focused on medical applications, Synchron's real-world testing has shown movement toward potential non-medical commercialization by allowing patients to post on social media,[47] interface with Apple's Vision Pro headset,[48] and interact with Amazon's Alexa assistant.[49]

---

40. *See* Suseendrakumar Duraivel et al., *High-Resolution Neural Recordings Improve the Accuracy of Speech Decoding*, 14 NATURE COMMC'NS, Nov. 6, 2023, at 1, 10 (discussing research into the use of neural signals for speech decoding in patients with neurodegenerative disorders).

41. Kaylo T. Littlejohn et al., *A Streaming Brain-to-Voice Neuroprosthesis to Restore Naturalistic Communication*, 28 NATURE NEUROSCIENCE, 2025, at 902, 909–10.

42. *See* Wing-kin Tam et al., *Human Motor Decoding from Neural Signals*, 1 BMC BIOMEDICAL ENG'G, 2019, at 1.

43. *See generally* DESNEY S. TAN & ANTON NIJHOLT, BRAIN-COMPUTER INTERFACES 10 (2010) (discussing the use of brain signals to control computers in place of physical movement).

44. *See* Synchron First U.S. BCI Implant, *supra* note 5.

45. Zhi-Ping Zhao et al., *Modulating Brain Activity with Invasive Brain-Computer Interface*, 13 BRAIN SCI., 2023, at 1.

46. Tim Brinkhof, *How Neuralink's chief competitor is tapping into the brain without surgery*, FREETHINK (Dec. 12, 2024), https://www.freethink.com/biotech/synchron-bci [https://perma.cc/7ZYB-M7NF].

47. Press Release, Synchron, Synchron Announces First Direct-Thought Tweet, "Hello World," Using an Implantable Brain Computer Interface (Dec. 22, 2021, 20:27 EST), https://www.businesswire.com/news/home/20211222005557/en/Synchron-Announces-First-Direct-Thought-Tweet-"Hello-World"-Using-an-Implantable-Brain-Computer-Interface [https://perma.cc/M7AC-WHR7].

48. Press Release, Synchron, Synchron Announces First Use of Apple Vision Pro with a Brain Computer Interface (July 30, 2024, 8:00 AM EST), https://www.businesswire.com/news/home/20240730923591/en/Synchron-Announces-First-Use-of-Apple-Vision-Pro-with-a-Brain-Computer-Interface [https://perma.cc/3JST-H58W].

49. Press Release, Synchron, Synchron Announces First Use of Amazon's Alexa with a Brain Computer Interface (Sept. 16, 2024, 8:00 AM EST), https://www.businesswire.com/news/home/20240916709941/en/Synchron-Announces-

This direct neural connection raises significant privacy concerns, even in controlled therapeutic settings. BCI systems that enable motor control and communication must process and interpret a wide range of neural signals—potentially capturing data beyond what is strictly necessary for physical movement, speech, or device control.[50] As these technologies become more sophisticated, the line between therapeutic use and broader neural monitoring begins to blur.[51] This technical reality creates privacy implications that existing medical device regulations may not adequately address.

The evolution of BCIs for motor control and communication reflects a broader pattern in neural technology development: tools originally designed for medical use increasingly show potential for broader human enhancement and commercial applications. While restoring motor function and communication remains the primary goal, the underlying capability—decoding, interpreting, and acting on neural signals—establishes the foundation for more expansive use cases.[52] The success of clinical applications has accelerated interest in expanding BCI functionality beyond healthcare, particularly as private companies seek to commercialize these technologies.[53] This shift from medical innovation to consumer adoption underscores the limitations of traditional medical device regulations in addressing the risks of the emerging BCI market.

B. Sensory Reconstruction and Restoration

BCIs have made significant progress in visual data processing and reconstruction. Early studies established the feasibility of using brain activity to identify specific natural images by showing that functional magnetic resonance imaging (fMRI) could be used

First-Use-of-Amazon's-Alexa-with-a-Brain-Computer-Interface [https://perma.cc/5Y7Y-QTJA].

50. *See* Usman Salahuddin & Pu-Xian Gao, *Signal Generation, Acquisition, and Processing in Brain Machine Interfaces: A Unified Review*, 15 FRONTIERS IN NEUROSCIENCE, Sept. 12, 2021, at 7–11.

51. *See* Yuste et al., *supra* note 36, at 161.

52. Zara Abrams, *The Future of Brain-Computer Interfaces*, IEEE PULSE (Jan. 25, 2023), https://www.embs.org/pulse/articles/the-future-of-brain-computer-interfaces/ [https://perma.cc/JS4Z-3KGS].

53. *See* U.S. GOV'T ACCOUNTABILITY OFF., SCIENCE & TECH. SPOTLIGHT: BRAIN-COMPUTER INTERFACES 1 (2022), https://www.gao.gov/assets/880/874491.pdf [https://perma.cc/2QJU-EJVE] (describing emerging nonmedical applications of BCIs in the workplace, national defense, and entertainment, and noting increased private-sector involvement).

to determine which image a person was viewing from a set of photographs based solely on their neural activity.[54]

Recent technological advances have significantly enhanced the accuracy and sophistication of neural decoding techniques. A 2023 study reported approximately 90 percent accuracy in identifying mental images using advanced machine-learning algorithms.[55] The researchers demonstrated the ability to reconstruct mental images in great detail and suggested that similar methods could potentially be used to access and reconstruct other forms of mental content.[56] In particular, they proposed that these techniques could be applied to the reconstruction of imagery from memory, imagination, and dreams—not only from actively perceived images.[57]

With fMRI scanners costing up to three million dollars and weighing as much as seventeen tons,[58] current reconstruction techniques' reliance on such machines limits their potential for widespread use. Commercial interests in these applications could drive efforts to overcome this technical limitation by incentivizing companies to explore alternative recording methods. Despite this constraint, their increasing accuracy raises profound privacy concerns by enabling access to thoughts and mental processes that individuals reasonably expect to remain private. The increasing accuracy of these reconstruction techniques, combined with advances in artificial intelligence, suggests that future systems might be capable of accessing and interpreting an even broader range of mental content.[59]

While sensory reconstruction techniques focus on extracting data from the brain, there have also been advancements in delivering sensory input back into it. Neuralink's Blindsight project, which received FDA Breakthrough Device designation in September 2024, aims to restore vision in blind individuals.[60] Similar BCIs—such as the earlier Cortigent Argus II[61] and its

54. *See* Bing Du et al., *fMRI Brain Decoding and Its Applications in Brain-Computer Interface*, 12 BRAIN SCI., 2022, at 1 (surveying previous experimentation with fMRI based mental image decoding).

55. Koide-Majima et al., *supra* note 9, at 358–61.

56. *Id.* at 361.

57. *Id.*

58. *Researchers Create MRI Scanner Parts in Just Four Days*, N.Y.U. LANGONE HEALTH (Dec. 8, 2023), https://nyulangone.org/news/researchers-create-mri-scanner-parts-just-four-days [https://perma.cc/NPB6-D3JW].

59. *See generally* Du et al., *supra* note 54.

60. Jessica Hagen, *Elon Musk's Neuralink device Blindsight gets FDA breakthrough device designation*, MOBIHEALTHNEWS (Sept. 19, 2024, 12:41), https://www.mobihealthnews.com/news/elon-musks-neuralink-device-blindsight-gets-fda-breakthrough-device-designation [https://perma.cc/XL73-YSNW].

61. *Argus II*, CORTIGENT, https://www.cortigent.com/argus-ii [https://perma.cc/RK6V-6ECS] [hereinafter *Argus II*].

successor Orion[62]—have already demonstrated potential in restoring limited vision in patients with total loss of sight.[63] Touch restoration through BCIs presents additional challenges, but developments show promise. Research has demonstrated that electrodes implanted in the somatosensory cortex can induce realistic tactile sensations, allowing prosthetic limb users to regain a sense of touch.[64]

The sensory capabilities of BCIs carry profound implications. As sensory reconstruction techniques advance, the ability to access and interpret mental imagery raises fundamental questions about mental privacy. The prospect of decoding not only perceived images but also internally generated content—such as memories and imagined ideas—introduces serious privacy concerns.[65] Unlike traditional privacy violations requiring external data collection, neural decoding allows direct access to mental experiences previously considered entirely private.[66]

Similarly, the ability to deliver information directly into the brain raises questions about the control over that input and whether either the user or an external observer can verify the authenticity of the resulting experience.[67] It also introduces the risk of unrelated or unintended data being transmitted into the brain.[68] The capacity to access internal mental states and inject information directly into the mind marks a qualitative shift in the nature of privacy and autonomy—one that demands new frameworks for protection.

C. Memory Modification

Research into memory modification represents a significant shift from simply recording and decoding neural data to actively manipulating mental content. Studies have demonstrated the

62. *Orion*, CORTIGENT, https://www.cortigent.com/orion [https://perma.cc/E7DT-YJK6].

63. *See Argus II*, *supra* note 61; *see* Mark Harris, *Second Sight's Implant Technology Gets a Second Chance*, IEEE SPECTRUM (Aug. 15, 2023), https://spectrum.ieee.org/bionic-eye [https://perma.cc/R5Z3-JQ66].

64. *See* Sliman J. Bensmaia & Lee E. Miller, *Restoring Sensorimotor Function Through Intracortical Interfaces*, 15 NATURE REVS. NEUROSCIENCE, Apr. 17, 2014, at 313, 313, https://doi.org/10.1038/nrn3724 [https://perma.cc/UL7K-QHWJ].

65. *See generally* Tesink et al., *supra* note 17 (discussing the privacy implications of memory retrieval).

66. *Id.*

67. *See* Marcello Ienca & Pim Haselager, *Hacking the Brain: Brain-Computer Interfaces and the Ethics of Neurosecurity*, 18 ETHICS AND INFO. TECH. 117, 126–28 (2016) (exploring the concept of "brain-hacking" where malicious actors could gain unauthorized access to neural information, manipulate sensory experiences, and compromise the authenticity of perceptions delivered through BCIs).

68. *Id.* at 122.

ability to selectively weaken or strengthen specific memories through targeted brain stimulation.[69] Using non-invasive techniques, researchers have successfully altered fear memories and emotional responses in controlled settings.[70] While these capabilities are promising for treating conditions such as post-traumatic stress disorder (PTSD),[71] they also raise concerns about the potential mental manipulation that entirely bypasses consent.

Recent advances in memory modification technologies (MMTs) have shown increasing precision in targeting specific memories.[72] Researchers have successfully used these techniques to alter both the emotional valence and factual content of memories, suggesting the potential for more substantial manipulation.[73] The ability to modify not only how memories feel but also their content challenges fundamental assumptions about the reliability of human memory and the authenticity of personal experience.[74]

The therapeutic potential of MMTs extends beyond treating trauma-related conditions. Research suggests these technologies may have applications in addiction treatment, phobia resolution, and even the enhancement of learning and memory formation.[75] However, this broad utility also raises concerns about the line between treatment and enhancement. The same MMTs that can help patients overcome trauma might also be used to enhance memory or selectively edit autobiographical experiences.[76]

The development of memory modification capabilities presents distinct challenges for protecting privacy and autonomy. Unlike neural recording technologies that only access mental content, MMTs can fundamentally alter the substance of consciousness itself.[77] The ability to manipulate the neural processes underlying personal identity and autobiographical memory introduces risks far beyond traditional privacy concerns. The distinction between therapeutic and enhancement applications becomes increasingly unclear as these technologies grow more precise and accessible.[78]

---

69. Borgomaneri et al., *supra* note 10, at 335–36.

70. *Id.* at 336–40.

71. *Id.* at 342.

72. Przemysław Zawadzki & Agnieszka K. Adamczyk, *To Remember, or Not to Remember? Potential Impact of Memory Modification on Narrative Identity, Personal Agency, Mental Health, and Well-being*, 35 BIOETHICS 891, 893–94 (2021).

73. *Id.*

74. Shawn Zheng Kai Tan & Lee Wei Lim, *A Practical Approach to the Ethical Use of Memory Modulating Technologies*, 21 BMC MED. ETHICS, Sept. 18, 2020, at 1, 5.

75. *See* Borgomaneri et al., *supra* note 10.

76. Zawadzki & Adamczyk, *supra* note 72, at 895–96.

77. *See* Muriel Leuenberger, *Memory Modification and Authenticity: A Narrative Approach*, 15 NEUROETHICS, Feb. 16, 2022, at 1, 7–9.

78. *See* Zawadzki & Adamczyk, *supra* note 72.

As memory modification moves from medical research toward potential commercial applications, the need for frameworks protecting both mental privacy and cognitive autonomy becomes more urgent.

D. Decision-Making Prediction and Modulation

Arguably the most concerning capability of BCIs is their potential to predict and influence conscious decision-making. Studies have shown that neural activity can be used to anticipate decisions up to eleven seconds before a person becomes consciously aware of their choice.[79] These predictive BCIs have achieved high precision with some studies achieving over 80% accuracy in predicting binary choices prior to conscious awareness.[80]

Beyond predicting decisions, researchers have also demonstrated the ability to influence decision-making processes. By stimulating specific brain regions, non-invasive BCIs can alter moral judgments, risk assessment, and financial decision-making.[81] The ability to influence such fundamental aspects of human cognition raises profound questions about preserving independent decision-making as these technologies advance.[82]

Combining predictive capabilities with decision-making influence creates previously impossible risks to human autonomy. Unlike typical forms of influence or persuasion—where duress or coercion are generally involved in consciously changing someone's behavior[83]—neural manipulation operates below the threshold of conscious awareness and could bypass normal psychological defense mechanisms.[84] This capability fundamentally challenges the understanding of autonomous choice and personal agency.

The development of predictive and influential capabilities in BCIs represents a major change in the relationship between humans and computers. While decision-making prediction and modulation technologies are currently limited to research settings,[85] the potential for their commercial application raises serious concerns about mental autonomy and privacy protection. Traditional privacy frameworks, designed to protect against

79. Koenig-Robert & Pearson, *supra* note 12, at 2.

80. Yajing Si et al., *Predicting Individual Decision-Making Responses Based on Single-Trial EEG,* NEUROIMAGE, 2020, at 1, 6–7.

81. Brunyé, *supra* note 11.

82. Yuste et al., *supra* note 36, at 161.

83. *See* Robert Noggle, *The Ethics of Manipulation*, in *The Stanford Encyclopedia of Philosophy* (rev. 2022), https://plato.stanford.edu/archives/fall2025/entries/ethics-manipulation [https://perma.cc/K4SF-6R2F].

84. Mohamed Elgendi et al., *Subliminal Priming—State of the Art and Future Perspectives*, 8 BEHAVIORAL SCI., May 30, 2018, at 1.

85. *See* Maiseli et al., *supra* note 34.

unauthorized data collection and disclosure, may prove inadequate against technologies that can both predict and influence cognitive processes before conscious awareness. As these capabilities advance, the need for new legal frameworks that specifically address neural privacy and cognitive liberty becomes increasingly urgent.

E. Commercial Applications and Development

The development of BCI technology has begun shifting from academic and medical research toward commercial applications.[86] Major technology companies and startups are increasingly investing in BCI development, signaling the intent to introduce these technologies into the consumer market.[87] This period of commercialization has coincided with drastic improvements in neural recording technology and artificial intelligence, enabling increasingly sophisticated neural interfaces.[88]

The commercial BCI landscape has become increasingly competitive, with multiple companies pursuing different technological approaches. Meta has invested heavily in developing non-invasive BCIs, focusing on applications such as alternative typing methods and enhanced interaction with augmented reality devices.[89] Its newest BCI project, Brain2Qwerty, transitions from using EEG for measurement to magnetoencephalography (MEG).[90] The shift to MEG allows for significantly improved accuracy compared to EEG based counterparts.[91] Meta's emphasis on non-invasive BCI technologies suggests a path toward widespread consumer adoption of BCIs.

Similarly, while Elon Musk's Neuralink has focused on medical applications, the company has expressed broader ambitions to enhance human cognitive capabilities.[92] The trend toward

86. *Id.*

87. Khorram, *supra* note 35.

88. *See generally* Xiayin Zhang et al., *The Combination of Brain-Computer Interfaces and Artificial Intelligence*, ANNALS OF TRANSLATIONAL MED., June 15, 2020, at 1 (discussing the application of artificial intelligence to BCI systems).

89. *Imagining a new interface*: *Hands-free communication without saying a word*, META (Mar. 30, 2020), https://tech.facebook.com/reality-labs/2020/3/imagining-a-new-interface-hands-free-communication-without-saying-a-word/ [https://perma.cc/667G-P2YU].

90. Sandeep Chatterjee, *Typing with Thoughts: Brain2Qwerty by Meta*, MEDIUM (Feb. 10, 2025), https://medium.com/@ML-today/typing-with-thoughts-brain2qwerty-by-meta-1256f2adcf57 [https://perma.cc/GNP3-A97W].

91. *Id.*

92. Isobel Asher Hamilton, *Elon Musk believes AI could turn humans into an endangered species like the mountain gorilla*, BUSINESS INSIDER (Nov. 26, 2018, 05:55 AM

commercialization has accelerated with Synchron's partnering with Nvidia, a leading technology company specializing in artificial intelligence and computing. This collaboration aims to integrate Nvidia's Holoscan artificial intelligence platform into Synchron's future BCI systems.[93] Synchron claims Holoscan's capabilities have "the potential to transform neuroprosthetics, cognitive expression, and seamless interaction with digital devices."[94]

Beyond major technology companies, BCI-focused startups are already introducing consumer applications that raise significant privacy concerns. For example, Emotiv markets its non-invasive BCI for "neuromarketing"—claiming to "[measure] consumers' brain waves. . . [to] see with unprecedented accuracy what truly captures attention, evokes emotion, and drives decision-making."[95] This application demonstrates how BCIs can be used to influence consumer behavior in ways that current privacy frameworks may not adequately address. Another startup, Neurable, has partnered with audio manufacturer Master & Dynamic to release headphones with integrated EEG sensors designed to provide users with insights into their mental health and productivity.[96] Launched in 2024, this product is one of the first mass-market BCI devices, and it is representative of Neurable's mission to "seamlessly integrate [BCIs] into daily life."[97]

The BCI market is expected to grow substantially over the next several years, with one projection estimating the global market to grow from 2.3 billion dollars in 2024 to 4.5 billion dollars by 2029.[98] The rapid commercialization of BCIs—coupled with their expanding capabilities—poses challenges for privacy and autonomy protection and highlights the limitations of current regulatory frameworks.

MT), https://www.businessinsider.com/elon-musk-ai-could-turn-humans-into-endangered-species-2018-11 [https://perma.cc/G7B9-WUN9].

93. Press Release, Synchron, Synchron to Advance Implantable Brain-Computer Interface Technology with NVIDIA Holoscan (Jan. 13, 2025, 13:30 EST), https://www.businesswire.com/news/home/20250113376337/en/Synchron-to-Advance-Implantable-Brain-Computer-Interface-Technology-with-NVIDIA-Holoscan [https://perma.cc/9JT3-8Q66].

94. *Id.*

95. *Consumer Research*, EMOTIV, https://www.emotiv.com/pages/consumer-research [https://perma.cc/C9BW-J7RY].

96. Press Release, Neurable Inc., Neurable Inc. Launches First Smart Brain-Computer Interface Enabled Headphones for Consumer Market (Sept. 24, 2024, 08:00 AM EDT), https://www.businesswire.com/news/home/20240924893354/en/ [https://perma.cc/ZCN8-TRKZ].

97. NEURABLE, https://www.neurable.com/ [https://perma.cc/63Q7-J5BN].

98. Press Release, BCC Research, Brain-Computer Interface: Global Markets (Jan. 14, 2025), https://www.bccresearch.com/pressroom/ias/brain-computer-interface:-global-markets [https://perma.cc/HMT7-XCNU].

The current wave of commercialization has entered a significant stage. In May 2025, Synchron announced a collaboration with Apple through Apple's newly developed *Brain-Computer Interface Human Interface Device (HID) Protocol*—a framework designed in-house to recognize neural input as a native interaction modality across its operating systems.[99] Apple's historical pattern of converting strategic partnerships into acquisitions—as seen with Siri (originally owned by SRI International),[100] Touch ID (originally owned by AuthenTec),[101] and Beats[102]—suggests this engagement may signal deeper ambitions. If past trends hold, we may be only a few product cycles from Apple's next marketing line: "Vision Pro. Now with your brain."

II. LIMITATIONS OF CURRENT LEGAL FRAMEWORKS

The current legal framework for neural data protection in the United States comprises a fragmented mix of federal and state regulations, most of which predate modern BCI technology. At the federal level, the Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) share oversight in this area.[103] Despite their differing roles, neither can adequately regulate BCIs in the consumer context because of the mismatches between their regulatory authority and the technology's capabilities. Beyond conventional privacy concerns around data collection and processing, these technologies introduce distinct risks to mental autonomy that require new protective frameworks.

While Colorado and California have pioneered legislation recognizing neural data within their privacy frameworks,[104] these approaches remain insufficient for addressing the new challenges

99. Omar Ford, *Apple Jumps into the Brain-Computer Interface Market with Synchron Collaboration*, MD + DI (May 13, 2025), https://www.mddionline.com/neurological/apple-jumps-into-the-brain-computer-interface-market-with-synchron-collaboration [https://perma.cc/6X2P-4R7T].

100. Jenna Wortham, *Apple Buys a Start-Up for Its Voice Technology*, N.Y. TIMES (Apr. 29, 2010), https://www.nytimes.com/2010/04/29/technology/29apple.html [https://perma.cc/69ZF-GZHT].

101. Poornima Gupta & Sinead Carew, *Apple buys mobile security firm AuthenTec for $356 million*, REUTERS (July 27, 2012, 17:04 MDT), https://www.reuters.com/article/world/americas/apple-buys-mobile-security-firm-authentec-for-356-million-idUSBRE86Q0KF/ [https://perma.cc/Z3PD-SMPJ].

102. Press Release, Apple Inc., Apple to Acquire Beats Music & Beats Electronics (May 28, 2014), https://www.apple.com/newsroom/2014/05/28Apple-to-Acquire-Beats-Music-Beats-Electronics/ [https://perma.cc/6VYY-KPZ2].

103. Henry Fisher, *The Challenges of Regulating Brain-Machine Interfaces*, REGUL. REV. (Nov. 24, 2022), https://www.theregreview.org/2022/11/24/fisher-the-challenges-of-regulating-brain-machine-interfaces/ [https://perma.cc/CV4E-VAW4].

104. H.B. 24-1058, 74th Gen. Assemb., 2th Reg. Sess. (Colo. 2024); S.B. 1223, Reg. Sess. (Cal. 2024).

that advanced BCI technology presents. State=level regulation of neural data privacy remains in its infancy, with most jurisdictions lacking specific protections for neural information. This fragmented approach leaves significant gaps in addressing the unique risks associated with BCIs.

A. Federal Regulation

1. Health Insurance Portability and Accountability Act

HIPAA provides the primary federal protection for medical information, including neural data collected in healthcare settings.[105] Under the HIPAA Privacy Rule, covered entities must protect all individually identifiable health information, which necessarily includes neural recordings, brain imaging data, and other BCI-generated data when collected for medical purposes.[106] The HIPAA Security Rule further requires appropriate technical, physical, and administrative safeguards for electronic protected health information, including neural data in electronic health records.[107]

However, HIPAA's scope is limited to these covered entities.[108] This includes healthcare providers, such as doctors, hospitals and clinics, health insurance plans, healthcare clearinghouses that process medical data, and the businesses that work with these entities.[109] HIPAA's limited scope becomes problematic as BCI technology moves beyond traditional medical settings into the general consumer market. For example, neural data collected by consumer BCI devices for entertainment, productivity, or personal wellness fall outside HIPAA's protection, even when such data would reveal sensitive medical information.[110]

Moreover, HIPAA's focus on privacy means it cannot address the other risks posed by BCIs, particularly with decision-making interference and the overriding of autonomy. The law's traditional conception of health information privacy centers on confidentiality and controlled sharing of medical data rather than protecting against direct manipulation of mental processes or safeguarding

105. HHS, *supra* note 15.
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *See* Kristen Lee, *Wearable health technology and HIPAA: What is and isn't covered*, TECHTARGET (July 24, 2015), https://www.techtarget.com/searchhealthit/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/NAK2-C4YT].

cognitive liberty.[111] While robust for traditional privacy violations, HIPAA's enforcement mechanisms provide no remedies for harms that aren't directly related to privacy,[112] such as unauthorized neural influence or compromised mental autonomy. Given the ability of BCIs to access and influence neural processes, lawmakers may need to revise HIPAA's provisions for patient consent and data access rights.

2. Food and Drug Administration Oversight

The FDA's authority to regulate BCIs stems from the Food, Drug, and Cosmetic Act (FDCA). Under Section 201(h) of the FDCA, a "medical device" is defined as:

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article. . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease. . . or intended to affect the structure or any function of the body of man or other animals.[113]

This broad definition covers all invasive and non-invasive BCIs when used for medical purposes and other purposes that directly affect the body.[114]

Within the FDCA's framework, invasive BCIs are typically classified as Class III devices, requiring the most stringent controls and pre-market approval.[115] The FDA's regulatory approach to these devices focuses primarily on evaluating safety and efficacy within the definition of a "medical device," without oversight for broader implications for neural privacy and autonomy. Non-invasive BCIs are typically classified as Class II devices, making them subject to specific controls but with less stringent requirements than Class III devices.[116] This tiered approach reflects the relative risks associated with different types of BCIs in medical applications.

---

111. *See generally* Mark A. Rothstein, *The End of the HIPAA Privacy Rule?*, 44 J.L. MED. & ETHICS 352, 354–55 (2016).

112. *See* HHS, *supra* note 15.

113. *See* FDA, *How to Determine if Your Product is a Medical Device*, https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device [https://perma.cc/RQ73-4EUA].

114. *See id.*

115. *See* 21 C.F.R. pt. 882 (2023) (classifying neurological devices; while BCIs are not listed explicitly, comparable implantable systems are Class III and external EEG-based systems are Class II).

116. *Id.*

However, the FDA's regulatory authority is less clear when BCIs are marketed for non-medical purposes. Consumer devices marketed primarily for entertainment, productivity, or general wellness may fall outside the FDA's scope.[117] This becomes problematic as the line between the medical and non-medical applications of BCI technology becomes increasingly blurred. A device marketed for entertainment or productivity might still be capable of collecting sensitive neural data or influencing cognitive processes but may escape FDA oversight if it is not intended for medical use under the FDCA's definition of a medical device or does not clearly influence bodily functions.[118]

Furthermore, the FDA's focus on physical safety and medical efficacy may not adequately address the unique privacy and autonomy risks posed by BCI technology. While the agency can evaluate the physical risks of BCI implants or the accuracy of neural measurements,[119] it lacks apparent authority and established frameworks to assess risks to mental privacy or cognitive liberty. This limitation becomes particularly problematic as BCIs develop capabilities for actively influencing neural activity rather than just recording.[120]

3. Federal Trade Commission Regulatory Authority

The FTC has broad authority to protect consumers from unfair or deceptive practices involving personal data, exercising this power through Section 5 of the FTC Act.[121] The Commission's traditional consumer protection framework emphasizes transparency and consent in data collection and use.[122] However, this framework lacks specific provisions for neural data privacy or mental autonomy.[123]

---

117. *See* FDA, Guidance Document, *General Wellness: Policy for Low Risk Devices* (Sept. 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices [https://perma.cc/NNU5-4UE7] (explaining that products intended only for general wellness, such as those promoting relaxation, mental acuity, or stress management, are not actively regulated as medical devices).

118. *See id*.

119. *See* 21 U.S.C. § 360c(a)(2)(A)–(B) (defining "safety" and "effectiveness" as related to physical risks and performance characteristics).

120. *See* Yuste et al., *supra* note 36, at 161–62 (discussing regulatory gaps in neural technology oversight).

121. FTC, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* (revised July 2025), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/3J9N-RRZ2].

122. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235–37 (2015).

123. *See id*.

The FTC's enforcement authority primarily addresses deceptive data collection and use practices, requiring companies to adhere to their stated privacy policies and obtain informed consent for data collection.[124] In past privacy enforcement actions, the Commission has focused on unauthorized data sharing, inadequate security measures, and deceptive privacy notifications.[125] This post hoc enforcement approach—relying primarily on consent decrees issued after violations are discovered rather than through ex ante regulation—may prove insufficient for addressing the unique risks posed by BCI technology.[126]

While the FTC has authority over emerging commercial technologies involving personal data collection, the Commission did not design its current regulatory framework around BCI technology and its capabilities.[127] The Commission's primary focus on protecting consumers from economic harm may not adequately capture the full range of potential harms from neural data collection and manipulation.[128] For instance, while the FTC can address misleading claims about data collection practices,[129] it may struggle to regulate neural influence over consumer decision-making without a clear economic impact.

The FTC's existing privacy protection frameworks are also unable to contend with the speed at which BCI technology can operate. Since neural data potentially enables influence over decisions before conscious awareness occurs, traditional notice-and-consent mechanisms become inadequate.[130]

124. *See id*. at 2235–36.

125. *Id*. at 2239–41.

126. *Id*. at 2242.

127. *Id.* at 2246–47.

128. *See* Becky Chao et al., *Enforcing a New Privacy Law,* NEW AMERICA (Nov. 20, 2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/ [https://perma.cc/9RXN-WALM].

129. Press Release, Kristen Cohen, Acting Associate Director, FTC Division of Privacy & Identity Protection , Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data (July 12, 2022), https://www.presidency.ucsb.edu/documents/white-house-press-release-location-health-and-other-sensitive-information-ftc-committed [https://perma.cc/V3WF-FMY3].

130. Anita S. Jwa & Russell A. Poldrack, *Addressing Privacy Risk in Neuroscience Data: From Data Protection to Harm Prevention,* J. L. AND BIOSCIENCES, Sept. 4, 2022, at 1, 6–7.

B. State Privacy Laws

1. Colorado Privacy Act

The 2024 neural data privacy amendment to the CPA represents the first explicit inclusion of neural data as a protected form of biometric data at the state level.[131] The act defines neural data 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."[132] This definition encompasses both medical and non-medical applications of BCI technology, marking a significant departure from HIPAA's healthcare-focused approach.

Under the CPA's framework, data controllers[133] must obtain specific, informed consent before collecting or processing sensitive data,[134] which includes neural data.[135] The act also mandates enhanced transparency measures, requiring detailed disclosures about the purposes of sensitive data collection and the specific types of data collected.[136] Data controllers must also specify whether and how they will combine neural data with other personal information to create profiles about individuals.[137]

The CPA grants Colorado residents substantial rights over their personal data, including the right to access, correct, delete, and obtain a copy of collected data.[138] Additionally, the act imposes heightened security requirements for storing and transmitting sensitive data.[139] The CPA also requires protection assessments for collecting and using personal data.[140] However, the neural data amendment does not provide specific guidance for assessing the unique risks posed by BCI technology.

While the CPA represents a significant step forward in recognizing neural data privacy, its framework remains focused on traditional data protection concerns that do not address the unique challenges posed by BCI technology. The act does not address the potential for direct manipulation of brain function, interference

131. Sigal Samuel, *Your brain's privacy is at risk. The US just took its first big step toward protecting it*, VOX (Apr. 18, 2024, 10:12 AM MDT), https://www.vox.com/future-perfect/24078512/brain-tech-privacy-rights-neurorights-colorado-yuste [https://perma.cc/JDK7-8PH6].

132. COLO. REV. STAT. § 6-1-1303(16.7) (2025).

133. *Id.* § 6-1-1303(7).

134. *Id.* § 6-1-1308(7).

135. *Id.* § 6-1-1303(24)(d) (biological data encompassing neural data).

136. *Id.* § 6-1-1308(1)(a).

137. *Id.* § 6-1-1308(2).

138. *Id.* § 6-1-1306(1)(a–e).

139. *Id.* § 6-1-1308(5).

140. *Id.* § 6-1-1309.

with conscious decision-making, or protection of psychological continuity. Furthermore, although the law requires data protection assessments, it provides no specific criteria for evaluating the distinctive risks associated with BCI applications. This gap leaves companies without clear guidance for assessing and mitigating the privacy and autonomy risks that BCIs present. Additionally, the CPA requires data controllers to "comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities,"[141] creating a pathway for government entities to access neural data collected by private businesses. This provision creates significant concerns about potential state access to intimate neural information without the specific protections that would apply to direct government collection of such data.

2. California Consumer Privacy Act

The CCPA was similarly amended in 2024 to recognize neural data as sensitive personal information.[142] The act defines neural data 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."[143] By excluding inferred neural information, California's definition creates a narrower and more precise scope than Colorado's approach—focusing exclusively on direct measurements of neural activity.

The CCPA's framework establishes a comprehensive set of rights and obligations regarding neural data processing.[144] Businesses must provide detailed privacy notices specifying their data collection and usage practices, including whether they use such data for automated decision-making or profiling.[145] California residents can also opt out of the sale or sharing of their neural data and limit the use and disclosure of neural data to purposes necessary to provide requested services.[146] The CCPA imposes additional restrictions on neural data collected from minors, requiring opt-in consent for individuals under 16 and parental consent for those under 13.[147]

---

141. *Id.* § 6-1-1304(3)(a)(2).

142. Jessica Hamzelou, *A new law in California protects consumers' brain data. Some think it doesn't go far enough*, MIT TECH. REV. (Oct. 4, 2024), https://www.technologyreview.com/2024/10/04/1104972/law-california-protects-brain-data-doesnt-go-far-enough/ [https://perma.cc/EF3B-WXXL].

143. CAL. CIV. CODE § 1798.140(ae)(1)(G)(ii) (West 2025).

144. *Id.* §§ 1798.100, 1798.120, 1798.140(ae)(1)(G)(ii), 1798.185.

145. *Id.* §§ 1798.100(a)(2), (b), 1798.185(a)(15).

146. *Id.* §§ 1798.120(a), 1798.121(a).

147. *Id.* § 1798.120(c).

Under the CCPA, businesses must implement reasonable security measures designed specifically to protect neural data, considering its unique sensitivity and potential for misuse.[148] However, the law's business purpose exceptions potentially create significant gaps in protection.[149] Under these exceptions, businesses may collect and process neural data without explicit consent when "reasonably necessary and proportionate" to provide requested services or other "disclosed purposes that [are]compatible with the context in which the personal information was collected."[150] This broad exception could allow companies to justify extensive neural data collection for service improvement, testing, internal research, and other purposes.[151] The breadth of these exceptions becomes particularly concerning in the context of BCIs, where even basic device functionality may require access to intimate forms of neural data.[152]

Similar to the CPA, California's approach focuses primarily on traditional data privacy principles such as notice, consent, and control rights. While the CCPA provides robust protections against unauthorized data collection and sharing, it does not address the potential for neural manipulation or the preservation of cognitive autonomy. The law's enforcement mechanisms, while substantial for conventional privacy violations, are inadequate for addressing novel harms arising from neural technology.[153] The CCPA's focus on commercial data practices leaves the broader implications of neural technology on individual autonomy and cognitive liberty unaddressed.

The limitations in these approaches underscore the need for a new framework that addresses both privacy and autonomy concerns. While Colorado and California have taken important first steps in recognizing the sensitive nature of neural data, effective protection requires also addressing the risk posed by techniques that can modify brain activity.

III. MINNESOTA'S PROPOSED FRAMEWORK FOR NEURAL PRIVACY PROTECTIONS

Minnesota Senate File 1240, introduced in the 2025-2026 legislative session,[154] would establish comprehensive protections

148. *Id.* §§ 1798.81.5, 1798.121(d).
149. *See id*. §§ 1798.105(d)(1), 1798.145(a).
150. *See id*. §§ 1798.100(c), 1798.105(d), 1798.145(a).
151. *See id*. §§ 1798.105(d)(1), 1798.145(a).
152. *See generally* Du et al., *supra* note 54 (discussing BCIs, their uses, and associated data).
153. Hamzelou, *supra* note 142.
154. Minn. S.F. 1240.

for neural privacy and autonomy through both civil and criminal provisions.[155] The legislation would create a multi-layered framework addressing both government and private sector use of neurotechnology.[156] Unlike Colorado and California's narrower approaches to neural data privacy, Minnesota's framework would establish specific rights, operational requirements, and enforcement mechanisms.[157]

Understanding Minnesota's approach requires examining three interconnected elements of neural privacy protection. S.F. 1240 begins by establishing fundamental restrictions on government entities, creating explicit rights to mental privacy and cognitive liberty through amendments to state data privacy law.[158] Building on these basic protections, the bill would impose requirements on private sector actors, including consent mechanisms and prohibitions on consciousness bypass techniques.[159] To give these protections practical force, the proposed legislation creates a comprehensive enforcement framework combining civil penalties, criminal sanctions, and public enforcement mechanisms.[160]

A. Government Restrictions and Public Rights

The foundation of Minnesota's framework lies in its explicit restrictions on government entities. S.F. 1240 contains two fundamental restrictions on government entities through amendments to Minnesota's data privacy statute.[161] First, it prohibits the collection of data transcribed directly from brain activity without informed consent, creating an explicit "right to mental privacy."[162] This restriction recognizes that government collection of neural data presents unique risks beyond traditional privacy concerns, such as potentially revealing thoughts, memories, and other purely internal mental states.

Second, the bill establishes a "right to cognitive liberty," barring government interference with "free and competent decision making" in neurotechnology decisions.[163] This provision moves beyond simple data protection to address potential manipulation or coercion in decisions about neural technology use. The dual focus

155. *Id.* §§ 2 subd. 5; 3 subd. 2.
156. *Id.* §§ 1, 2.
157. *Id.* §§ 1–4.
158. *Id.* § 1, subd. 1a.
159. *Id.* § 2.
160. *Id.* §§ 2, subd. 5–4.
161. *Id.* § 1, subd. 1a.
162. *Id.* § 1, subd. 1a(a).
163. *Id.* § 1, subd. 1a(b).

on "free" and "competent" decision-making suggests protection not just against overt coercion but also against subtle forms of influence that might compromise genuine autonomy.

These governmental restrictions create a baseline of protection against state intrusion into mental privacy. Further, recognizing that private actors may pose equal or more significant risks to neural privacy, the legislation establishes additional requirements for the commercial use of neurotechnology.

B. Private Sector Requirements and Restrictions

S.F. 1240 establishes comprehensive operational requirements for private entities centered on consent and transparency. Each time an individual connects to a BCI, the responsible company must provide specific notice of two elements: all potential uses of the collected data [by the company itself] and any third parties with whom it will share the data.[164] The legislation requires separate consent forms for each use and each third party, creating practical barriers to broad data sharing while ensuring granular control over neural information.[165]

The law establishes particularly stringent protections against "consciousness bypass," defined as "the use of neurotechnology to manipulate brain activity by applying electrical or optical stimuli without the conscious awareness of the person whose brain activity is being manipulated."[166] This definition addresses a unique risk of neural technology: the potential for manipulation below the threshold of conscious awareness. The legislation explicitly prohibits the use of consciousness bypass and invalidates any consent obtained through consciousness bypass techniques, preventing recursive use of the technology to authorize its own use.[167]

While S.F. 1240's protections are rigorous, the law leaves a narrow exception to allow consciousness bypass when necessary for a medical procedure, provided the patient gives informed consent prior to the procedure.[168] This exception acknowledges legitimate medical applications where consciousness bypass techniques may be medically beneficial, or where a medical procedure could be argued to involve such a technique, such as in memory modification

164. *Id.* § 2, subd. 3.
165. *Id.*
166. *Id.* § 2, subd. 1(c).
167. *Id.* § 2, subd. 4.
168. *Id.* § 2, subd. 4(b).

treatments for PTSD.[169] By requiring prior consent, the exception preserves these medical uses while keeping the framework's integrity.

While these substantive requirements establish clear rules for neural technology use, the effectiveness of any privacy framework ultimately depends on the robustness and viability of its enforcement mechanisms. The Minnesota legislation addresses this through a thorough system of penalties and enforcement authority.

C. Harm Recognition and Remedies

The legislation creates a multi-tiered enforcement system of civil penalties, criminal sanctions, and public enforcement authority. Companies that violate data collection consent requirements or consciousness bypass prohibition face civil penalties of up to $10,000 per incident.[170] The attorney general holds the authority to bring actions to recover these penalties, ensuring public enforcement capability.[171]

Beyond civil penalties, the bill significantly modifies existing computer crime statutes to address neural technology risks. It creates enhanced criminal penalties for unauthorized access to devices with BCIs, treating such access as a serious offense regardless of monetary damage.[172] This approach recognizes that traditional metrics of computer crime harm, often focused on financial damage, may not adequately capture the severity of neural privacy violations.

The framework also establishes specific criminal penalties for unauthorized access to BCI systems.[173] Such access constitutes a gross misdemeanor, placing it at a higher level than standard computer intrusion offenses.[174] Additionally, the law modifies existing computer damage statutes to treat any damage to BCI-equipped systems as a felony-level offense, regardless of monetary value.[175] This elevation of penalties reflects the legislature's recognition that compromising neural interfaces presents unique and serious risks beyond traditional cybersecurity concerns.

---

169. *See* Borgomaneri et al., *supra* note 10 (demonstrating that noninvasive brain stimulation can modulate fear memories without conscious awareness, suggesting therapeutic potential for PTSD treatment).

170. Minn. S.F. 1240, § 2, subd. 5.

171. *Id.*

172. *Id.* § 4, subd. 3.

173. *Id.* § 4, subd. 3(b–f).

174. *Id.*

175. *Id.* § 3, subd. 2(a)(2). The term "BCI-equipped systems" is used here to reflect this statutory phrasing.

This combination of civil penalties, criminal sanctions, and enhanced computer crime provisions creates significant consequences for neural privacy violations. However, the framework's practical implementation faces several technical, constitutional, and operational challenges that lawmakers must address.

IV. STRENGTHENING MINNESOTA'S FRAMEWORK

While Minnesota's proposed legislation provides a strong foundation for neural privacy protection, several aspects require refinement to ensure effective implementation. The bill's current form leaves significant gaps between its ambitious protections and practical enforceability. However, lawmakers may be able to address these gaps through specific modifications to the existing framework without fundamentally altering its protective structure.

Strengthening Minnesota's framework requires attention to several key areas of implementation. While groundbreaking, the framework's requirements for neural data protection and consciousness bypass prevention need specific technical standards to guide compliance and enforcement. Beyond technical specifications, the framework's consent mechanisms require more detailed procedures to ensure meaningful user control over neural data. Although the bill's enforcement provisions would create significant penalties, the provisions need more precise standards for violation detection and evidence preservation. Finally, the legislation must establish more detailed guidance for medical exceptions to ensure they do not become loopholes that undermine the broader protections.

A. Technical Implementation Standards

The legislation's requirements for neural data protection and consciousness bypass prevention lack specific technical standards for compliance. While the bill defines consciousness bypass as "the use of neurotechnology to manipulate brain activity by applying electrical or optical stimuli without conscious awareness,"[176] it provides no guidance on implementation. The current absence of clear technical standards may lead companies to implement widely varying protective measures, creating uncertainty and complicating compliance.[177]

176. *Id.* § 2, subd. 1(c).

177. *See* Alan Friel & Kyle Fath, *Federal Privacy Bill's Vagueness Threatens Ad-Supported Businesses*, BLOOMBERG L. (May 1, 2024, 2:30 AM MDT), https://news.bloomberglaw.com/us-law-week/federal-privacy-bills-vagueness-threatens-ad-supported-business [https://perma.cc/4B8C-L7QT].

Clear technical standards are particularly crucial given the unique risks of neural technology. Unlike traditional privacy violations that occur after data collection, neural manipulation can create immediate and potentially irreversible effects. The speed at which neural processes occur means that post hoc detection of violations may come too late to prevent harm.[178] This timing challenge reveals a fundamental limitation in traditional regulatory approaches that rely on after-the-fact enforcement. While existing privacy frameworks can address data breaches through investigations and penalties, the direct manipulation of neural processes may require a different regulatory paradigm emphasizing prevention rather than remediation. Developing appropriate technical standards to address this challenge will require close collaboration between neuroscientists, engineers, and policymakers.

The legislation's consciousness bypass provisions highlight this need for technical clarity. Companies must not only avoid intentional consciousness bypass but also prevent accidental or unauthorized neural influence. Without specific standards, companies lack guidance on what constitutes adequate protection against these risks.[179] Moreover, regulators and courts would have no clear benchmark for evaluating whether a company's protective measures are sufficient.

Clear technical standards would also facilitate consistent enforcement. The current framework creates significant penalties for violations but provides no standard way to detect or document them.[180] This ambiguity could make the bill's enforcement provisions difficult to implement effectively, potentially undermining its protective purpose. Beyond these technical specifications, lawmakers must also address the issues with the framework's consent mechanisms.

B. Enhanced Consent Requirements

While the Minnesota framework establishes important principles, its consent provisions require further development to ensure meaningful protection. The bill requires companies to obtain separate consent for each use of neural data and for each third

178. *See* Koenig-Robert & Pearson, *supra* note 12, at 7 (discussing how neural activity predicts decisions before conscious engagement).

179. *See* Yuste et al., *supra* note 36, at 161–62 (arguing that standards are needed to safeguard privacy and consent, agency and identity, equitable augmentation, and bias mitigation in neurotechnologies).

180. Minn. S.F. 1240 § 4.

party with whom they will share data.[181] However, the framework does not specify how companies should obtain and verify consent, particularly given the unique challenges of neural technology.

Traditional digital consent mechanisms prove inadequate in the context of neural technology. When a system can potentially influence decision-making processes, standard "click-through" consent provides insufficient protection. The recursive nature of neural influence—where the technology seeking consent could affect the consent decision itself—creates unique challenges that the current framework does not fully address.[182]

The temporal aspects of neural data collection further complicate consent issues. While BCIs could utilize external devices to obtain consent prior to activation, similar to traditional technologies, some BCIs may need to first process neural signals to then even display consent information to the user. Moreover, neural data collected during the consent process itself could reveal sensitive information, creating a paradox where data collection becomes necessary to obtain consent for data collection. The legislation needs to address these technical realities while maintaining meaningful consent requirements.

The medical exception to the consciousness bypass prohibition exemplifies these consent challenges most acutely. While the bill specifically states that "consent obtained by using a consciousness bypass is not informed consent,"[183] it provides no guidance on verifying that consciousness bypass technology did not influence the consent process. Medical providers need clear standards for documenting that consent was obtained without neural influence, especially when using therapeutic applications that may affect cognitive processes.

The framework also fails to address evolving consent issues over time. As BCIs become more sophisticated and potentially learn user preferences, the line between user-directed actions and system-influenced decisions may blur. The legislation should establish mechanisms for ongoing consent verification and periodic reauthorization of neural data collection to ensure continued user autonomy. While these consent challenges require careful attention, the framework's mechanisms for monitoring compliance and ensuring accountability are equally important.

---

181. *Id.* § 2, subd. 3.

182. *See* Ienca & Haselager, *supra* note 67, at 126–28 (discussing how BCIs can influence autonomy and decision-making, raising ethical concerns about the recursive nature of neural influence on consent).

183. Minn. S.F. 1240 § 2, subd. 4(b).

C. Practical Enforcement Challenges

S.F. 1240 creates significant penalties for violations but provides limited guidance on monitoring and verifying compliance. While the bill would authorize the attorney general to bring enforcement actions and establish civil penalties of up to $10,000 per incident,[184] it does not establish specific monitoring requirements or designate clear oversight authority for ongoing compliance verification.

This gap in compliance monitoring creates several practical challenges. Without designated oversight authority, companies lack clear guidance on who will evaluate their neural privacy protections or how such evaluations will occur. The legislation's focus on post-violation enforcement fails to create mechanisms for preventing violations through regular monitoring and compliance verification. This reactive approach proves particularly problematic given the potential irreversibility of neural privacy violations.

The framework also lacks provisions for independent verification of protective measures. While companies must implement protections against consciousness bypass and unauthorized data sharing, the legislation provides no mechanism for verifying the effectiveness of these protections before violations occur. Given the sophisticated nature of neural technology and the potential for subtle forms of influence, relying solely on post-hoc enforcement may prove insufficient to ensure meaningful protection.

Regular compliance auditing presents unique challenges in the neural technology context. Traditional privacy audits typically focus on data collection and storage practices,[185] but neural technology requires evaluating real-time protective measures against consciousness bypass and unauthorized influence. The legislation needs to establish specific requirements for compliance verification that address these unique aspects of neural technology.

While lawmakers can address these gaps in technical standards, consent mechanisms, and compliance monitoring through modifications to the existing framework, more fundamental challenges to neural privacy protection remain. Beyond these implementational issues, the Minnesota framework faces significant constitutional and practical barriers that may require broader structural solutions.

---

184. *Id.* § 2, subd. 5.

185. *See* FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business [https://perma.cc/585X-VSGA] (describing privacy audits as focusing on how organizations collect, store, and secure consumer data).

V. FUNDAMENTAL CHALLENGES TO NEURAL PRIVACY REGULATION

While specific modifications can address the Minnesota framework's implementation challenges, more fundamental barriers exist in establishing effective neural privacy regulation. These challenges stem not from the legislation's particular provisions but from inherent tensions between neural privacy protection and established legal principles. The framework's attempt to establish new rights and restrictions in response to neural technology confronts long-standing constitutional doctrines, jurisdictional limitations, and practical realities of modern technology platforms.

These fundamental challenges differ from the implementation issues addressed in Part V. While specific improvements can clarify technical standards and refine consent mechanisms, other barriers raise questions about whether traditional legal frameworks can meaningfully address neural privacy concerns. The concepts underlying neural privacy protection—mental integrity, cognitive liberty, protection against consciousness bypass—exist in tension with established legal principles about privacy, expression, and regulatory authority.

Understanding these fundamental challenges is crucial for developing workable approaches to neural privacy protection. Rather than simple gaps in the legislation, these issues represent structural barriers that may require rethinking basic assumptions about privacy law and constitutional rights. As neural technology advances, tensions between traditional legal frameworks and novel privacy concerns will only become more pronounced.

A. Constitutional Barriers

The Minnesota framework faces significant constitutional challenges. Its restrictions on neural data sharing and consciousness bypass potentially conflict with First Amendment protections for information sharing and expression.[186] Courts have consistently held that sharing truthful information, even when privacy-invasive, generally receives strong constitutional protection.[187] These holdings create tension for regulations seeking to restrict the sharing of neural data that individuals have consented to, even if those individuals lack a meaningful

186. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 567–70 (2011) (striking down restrictions on the sharing of medical prescription data).

187. *See, e.g.,* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496 (1975) (protecting publication of lawfully obtained, truthful information); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103–06 (1979) (holding that the state may not restrict publication of lawfully obtained information absent a compelling state interest); Bartnicki v. Vopper, 532 U.S. 514, 527–28 (2001) (protecting disclosure where publisher played no role in unlawful acquisition).

understanding of the scope or implications of the data they are allowing to be collected. However, unlike more traditional forms of personal data—such as consumer records or standard biometric information—neural data is much more intimate. This distinction could lead courts to reach a different conclusion regarding legal protections for neural data.

Precedent supporting the heightened protection of neural data can be found in *Carpenter v. United States*.[188] In *Carpenter*, the Supreme Court held that cell phone location data requires heightened protection compared to other forms of data due to its persistent and deeply revealing nature, as individuals carry a cell phone at almost all times.[189] Similarly, BCI technology has the potential to enable truly constant and highly invasive monitoring, reinforcing the need for enhanced legal safeguards. *Carpenter* also signaled a shift in the Court's approach to digital privacy by limiting the third-party doctrine, which traditionally allowed the government to obtain information shared with third parties without a warrant.[190] If this reasoning is applied to BCIs, access to neural data may be covered under similar Fourth Amendment protections.[191]

Beyond First and Fourth Amendment concerns, the framework's attempt to establish mental integrity as a fundamental right faces significant doctrinal challenges. While privacy rights have been recognized in various contexts, courts have been reluctant to expand fundamental rights beyond those with clear historical foundations.[192] The Supreme Court's recent emphasis on historical practice in recognizing fundamental rights suggests particular difficulty in establishing novel protections for neural privacy.[193] This challenge becomes particularly acute given the technological novelty of neural interfaces—courts applying historical analysis would find no clear analog for mental integrity rights in American legal tradition.

188. *See* Carpenter v. United States, 595 U.S. 296 (2018).

189. *Id.* at 314–16.

190. *Id.* at 306.

191. *See id*. at 311 (limiting the third-party doctrine where the government seeks data that provides an "intimate window into a person's life").

192. *See* Washington v. Glucksberg, 521 U.S. 702, 708–711 (1997) (holding that recognition of fundamental rights under due process is limited to those with a well-established historical foundation).

193. *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 215–18 (2022) (emphasizing historical analysis in fundamental rights recognition).

B. Jurisdictional Challenges

The Minnesota framework faces fundamental challenges arising from the structure of American federalism and the inherently interstate nature of modern technology. State attempts to regulate neural privacy would face potential preemption by federal authorities, particularly the FDA's comprehensive regulation of medical devices.[194] While states traditionally maintain broad authority to protect public health and safety, federal law explicitly preempts state requirements for medical devices that differ from federal requirements.[195]

This preemption creates major difficulties given the dual-use nature of BCI technology. Developers might use the technologies in a BCI for both therapeutic purposes regulated by the FDA and non-medical applications that states may seek to regulate. The Minnesota framework attempts to navigate this through its medical exception provisions, but the increasing convergence of therapeutic and enhancement applications makes clean distinctions difficult. A single neural interface might simultaneously provide medically necessary functions and enable activities the state seeks to regulate, creating direct conflicts with federal oversight.

Beyond federal preemption, the framework confronts practical jurisdictional challenges inherent in regulating modern technology platforms. Neural data collected in one state may be processed in another state or internationally, creating significant enforcement complications.[196] Traditional jurisdictional principles, focused on physical location and state borders, prove inadequate when addressing technology that operates through distributed systems and cloud computing.[197] A company might collect neural data from Minnesota residents while processing and storing that data entirely outside the state's borders, potentially creating complex jurisdictional questions.

Finally, attempts to regulate interstate neural data flows risk violating the Dormant Commerce Clause. Courts have consistently struck down state attempts to regulate internet activity that necessarily affects interstate commerce.[198] S.F. 1240's attempt to

194. *See* 21 U.S.C § 360k(a) (2018) (establishing federal preemption for medical device regulation).

195. *Id.*

196. *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168–72 (S.D.N.Y. 1997) (discussing jurisdictional challenges in regulating internet activity).

197. *See* Damon Andrews & John Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 368 (2013), https://www.marylandlawreview.org/volume-73-issue-1/personal-jurisdiction-and-choice-of-law-in-the-cloud [https://perma.cc/4QP5-U7HC].

198. *See American Libraries Ass'n*, 969 F. Supp. at 174.

control neural data collection and processing—activities that inherently cross state lines in modern computing environments—could face similar constitutional barriers.

These constitutional and jurisdictional challenges suggest that effective neural privacy protection may require solutions beyond traditional state legislation. While this framework provides an important foundation for protecting mental integrity and cognitive liberty, the fundamental barriers to state-level regulation indicate the need for a more comprehensive approach.

CONCLUSION

Minnesota's framework is one of the first attempts to confront what neural technology means for privacy and personhood. While Colorado and California treat neural data as another form of personal information, Minnesota goes much further. S.F. 1240 recognizes that neural privacy cannot be reduced to data management—that instead protecting the mind requires guarding both information and autonomy. Its creation of a right to mental integrity and limits on consciousness bypass establishes the outline of law built for the brain.

But this outline is fragile and imperfect. Technical standards and consent procedures can fill some gaps, but the harder questions still need answers. Neural privacy doesn't fit neatly into the mold of existing law—pressing at constitutional limits, preemption doctrine, and the boundaries of jurisdiction. Each friction point exposes the same fault: the legal system was built to govern actions, not cognition. The closer technology moves to the mind, the less those traditional frameworks hold.

Real protection will require more than technical fixes. It will need a framework that extends beyond state boundaries and statutory definitions—one that recognizes mental integrity as distinct from traditional notions of privacy. Minnesota's model remains incomplete, but it provides a necessary step toward acknowledging the mind as a protected domain of its own.

The problem is that the law is reactionary and recognizes harm only after it has taken shape. Neural technology removes the safe margin between cause and consequence. By the time the consequences are visible, BCIs will already influence the conditions under which they are judged. The frameworks that once defined harm and consent may not hold when the technology itself can shape perception. The question is whether the law can respond before the mind ceases to be the one place it assumed could never be reached.