Athens Journal of Law - Volume 11, Issue 4, October 2025 – Pages 671-686

Brain-Computer Interfaces at the Intersection of Innovation and U.S. Constitutional Law: A Literature Review and Case Law Perspective

*By Ryan A. Chang**

Brain-computer interfaces (BCIs) enable direct communication between the brain and external devices, offering transformative applications in assistive technology, communication, and cognitive enhancement. First conceptualised by UCLA scientist Jacques Vidal in 1973, BCIs have evolved from theoretical tools for medical rehabilitation to functioning systems with expanding non-therapeutic uses. As these technologies mature, they generate an unprecedented class of neurodata which may encompass one's thoughts, emotions, and memories. The highly personal nature of neurodata raises additional concerns about privacy, ownership, and consent. Its collection and use, especially when passive or involuntary, challenge existing legal frameworks and implicate key constitutional protections. This article explores the implications of BCI in context of the First, Fourth, and Fifth Amendments of the U.S. Constitution. Neurodata access could threaten freedom of thought, enable unreasonable searches, and bypass protections against self-incrimination. As BCIs move toward applications such as brain-to-brain communication, the urgency for legal safeguards grows. To address these challenges, the article advocates for integrated technological and legal protections, including encryption, user control, and legislation analogous to HIPAA. Recognizing emerging neurorights—such as cognitive liberty and mental privacy—will be critical to ensuring that BCI innovation advances without compromising fundamental rights and individual autonomy.

Keywords: *Brain-computer interfaces (BCIs); Constitutional rights; Mental privacy; Neurodata; Neurorights*

Introduction

Brain-computer interfaces (BCIs) are systems that enable direct communication between the brain and external devices. First proposed by UCLA computer scientist Jacques Vidal in 1973 as a means to merge the human brain with the processing power of computers[1], BCIs work by detecting neural signals, interpreting them, and translating them into commands that can control computers, prosthetics, or other devices. While there is no consensus on a definition of BCIs, there are a few defining characteristics that researchers and scholars agree upon which include the ability of the BCI device to 1) directly detect neural activity, 2) classify neural activity, 3) provide feedback in real-time or near real-time, and 4) provide user feedback that

*Undergraduate Researcher, Stanford University, Stanford, CA 94305, USA.
Email: rachang@stanford.edu.
[1]See Vidal (1973)

https://doi.org/10.30958/ajl.11-4-16 doi=10.30958/ajl.11-4-16

reflects whether a goal was successfully attained.[2] BCIs functionally interweave computer code and algorithms with the central nervous system, augmenting and sometimes replacing its functions.[3] Modern-day BCIs were initially developed for medical applications to help patients disabled by neurological diseases such as stroke or amyotrophic lateral sclerosis (ALS) regain some of their lost function.[4] BCIs are rapidly evolving to become smaller, less invasive, and have wireless connectivity.[5] Many scientists envision a future where BCIs can be used outside of the therapeutic setting to enable a new form of brain-to-brain communication–essentially telepathy–in healthy people.[6]

Mainstream adoption of BCIs will entail collecting, synthesizing, and translating brain data and, in the process, generating personal neurodata that would be transmitted from one BCI to another. The existence of this new unprecedented form of neurodata, potentially consisting of one's innermost private thoughts, memories, and emotions, opens the door for potential abuse around its use and raises new legal issues. Specifically, constitutional rights regarding unauthorised access to an individual's neurodata need to be addressed, as this is largely unregulated at the present. If others have unauthorized access to an individual's neurodata through BCI technology, in the United States, this could have legal ramifications regarding U.S. Constitutional Amendments 1 (the right of free speech, and therefore free thought), 4 (the right to privacy), and 5 (the right against self-incrimination). As BCI technology advances to allow new forms of communication, it would be essential to consider the impact of this technology on the rights of U.S. citizens protected by the above three Amendments. Safety features will need to be incorporated into the production of BCIs to help prevent violations of individual rights, and new laws will be necessary to ensure that this emerging technology complies with existing constitutional protection. Technological advances are inevitable, and BCIs will likely play a significant role in advancing the human mind, but it remains critical that this technology not be abused and that appropriate laws and regulation evolve with the technology.

Literature Review and Current State

Brain Computer Interface Technology

At its core, a brain–computer interface (BCI) provides a direct communication link between the human brain and an external device, translating neural signals into commands without relying on muscles or peripheral nerves.[7] Early BCIs were limited to basic tasks (e.g. moving a cursor or selecting letters), but the field has advanced rapidly. Modern BCI systems can decode complex mental intentions with increasing speed and accuracy. For example, rather than selecting letters one-by-one on a screen,

[2]See Burwell, Sample & Racine (2017).
[3]See Bublitz, Wolkenstein, Jox & Freidrich (2019).
[4]See Bai, Fong, Zhang, Chan &Ting (2020).
[5]See Green (2021).
[6]See Koala-Sterniuk (2021).
[7]See Zheng (2025).

researchers have demonstrated BCIs that decode attempted handwriting from neural activity in real-time, enabling paralysed users to text by thought at speeds approaching normal handwriting.[8] Other recent breakthroughs include BCI-driven speech prostheses (translating neural signals into synthesised speech or text), the real-time control of robotic limbs or computer cursors by motor cortex activity, and closed-loop systems that stimulate the brain to provide sensory feedback or influence mood.[9] Notable achievements in the last few years range from a wireless implanted BCI that restored a patient's ability to walk using an exoskeleton, to algorithms that interpret neural signals for communication in individuals with locked-in syndrome who cannot otherwise speak.[10] These advances highlight the growing sophistication of both BCI hardware (recording devices, electrodes) and software (signal decoding algorithms, often powered by machine learning).

Equally important has been the entry of industry and government actors into the BCI arena. Tech companies have made bold investments in neurotechnology: for instance, Facebook (Meta) announced a brain-typing project aiming to let users "type straight from your brain" at five times the speed of phone texting, and even acquired a startup working on neural signal wristbands to advance this goal.[11] Elon Musk's company Neuralink has been developing high-bandwidth implantable BCIs with flexible electrode threads, envisioning a future "symbiosis with artificial intelligence". Synchron, another BCI company, received FDA approval to test its Stentrode device in humans, a mesh electrode deployed via blood vessels, which has already enabled patients to control computer cursors by thought.[12] The U.S. military is also exploring BCIs; for example, the Defence Advanced Research Projects Agency has prototyped BCI systems for soldiers to control drone swarms "at the speed of thought".[13] Such commercial and governmental developments underscore that BCI technology is rapidly moving from laboratories toward real-world applications. Looking toward the future, researchers anticipate that BCIs will not only assist individual users but could network multiple brains together. Early experiments have realised direct brain-to-brain communication: a 2019 study, *BrainNet*, linked three people via EEG recordings and transcranial magnetic stimulation, allowing them to cooperatively play a Tetris-like game by exchanging thoughts in a rudimentary "social network of brains".[14] This proof-of-concept points toward a potential future of BCI-to-BCI communication, sometimes described as brain-to-brain interfaces (BBIs). While such applications remain nascent, they illustrate the far-reaching potential of BCIs and foreshadow the profound legal and ethical questions that arise when information flows directly from the mind.

[8]Edelman, Zhang, Schalk, Bunner, Muller-Putz, Guan & Be (2025).
[9]Ibid.
[10]See Myrick (2024).
[11]See George (2020).
[12]See Edelman, Zhang, Schalk, Bunner, Muller-Putz, Guan & Be (2025).
[13]See George (2020).
[14]See Liang, Stocco, Losey, Abernethy, Prat & Rao (2019).

Legal Implications of BCIs

The advent of BCIs raises unprecedented legal questions, especially as they intersect with fundamental rights in the U.S. Constitution. Recent papers have begun to explore how neurotechnology may challenge longstanding interpretations of the First, Fourth, and Fifth Amendments. Key issues include the right to cognitive liberty and freedom of thought (First Amendment), neuroprivacy and freedom from unreasonable searches of one's brain data (Fourth Amendment), and the privilege against self-incrimination with regard to one's own neural information (Fifth Amendment). The following section reviews the emerging literature in each domain.

First Amendment: Cognitive Liberty and Freedom of Thought

Commentators argue that BCIs implicate a basic "freedom of thought" interest that the First Amendment ought to protect, often referred to as the right to cognitive liberty. Cognitive liberty has been described as "the right and freedom to control one's own consciousness and electrochemical thought process"[15], and some scholars view it as a bedrock for all other expressive freedoms. Indeed, Ienca and others have characterised cognitive liberty as the "first, essential step" among proposed neurorights, reasoning that without the freedom to control one's own thoughts, rights like free speech, free exercise of religion, or freedom of association cannot truly exist.[16] Legal thinkers have pointed out that while the U.S. Constitution does not explicitly enumerate freedom of thought, the Supreme Court has recognised its importance in dictum; for example, noting that "First Amendment freedoms are most in danger when the government seeks to control thought".[17] The prospect of BCIs capable of reading or altering mental content has spurred calls to explicitly safeguard mental privacy and autonomy under First Amendment liberty.[18] If an employer or state actor could monitor an individual's neural activity (as one Chinese program reportedly did by having employees wear EEG-based caps to track alertness), scholars warn this would erode the absolute freedom to think one's own thoughts free from government intrusion, a freedom arguably implicit in the First Amendment's guarantee of conscience and expression.[19]

In addition to protecting the right to think, the First Amendment may be invoked to protect the right not to reveal one's thoughts. As BCIs generate neurodata, digitised records of brain activity that can contain the substance of one's private thoughts or intentions, some scholars contend that government access to this data would violate First Amendment protections, particularly the doctrine against compelled speech.[20] The argument, as articulated by Unger and others, is that forcing an individual to surrender the contents of their mind (for example, by handing over BCI-recorded data or submitting to a brain-scan interrogation) is akin to compelling them to speak against their will. The First Amendment has long been interpreted to include a right

[15]See Ienca (2021).
[16]See George (2020).
[17]Ibid.
[18]Ibid.
[19]Ibid.
[20]See Unger (2023a).

not to speak, preventing the government from coercing expression of beliefs or ideas.[21] By extension, scholars argue, it should also preclude the government from extracting a person's innermost thoughts via neurotechnology.[22] Unger proposes that the First Amendment offers more robust protection for personal thought data than the Fourth Amendment, precisely because accessing someone's neurodata intrudes on freedom of thought and opinion in a way that contradicts the spirit of free expression.[23] Thus, legal scholarship is beginning to frame cognitive liberty and mental privacy as First Amendment concerns, suggesting that BCIs may require courts to affirm an individual's right to keep their thoughts to themselves as an essential part of the freedom of mind that supports other expression rights.

Fourth Amendment: Neuroprivacy, Search and Seizure of Brain Data

BCI technology also challenges traditional notions of privacy under the Fourth Amendment, which guards against unreasonable searches and seizures. If a person's thoughts can be recorded and stored as data, does the government need a warrant to "search" your mind? Scholars increasingly insist that neurodata, the digital output of BCIs, potentially containing one's memories, intentions, or emotional state, must be treated as private information deserving the highest Fourth Amendment protection.[24] Unger argues that "neurodata unequivocally falls within the Fourth Amendment's protections" and that extending Fourth Amendment doctrine to cover brain-derived data is a "last stand" for privacy in the face of mind-reading technologies. He warns that if individuals cannot retreat into their own minds free from government surveillance, "then true solitude will become extinct".[25] This sentiment echoes the view that the mind is the ultimate inner sanctum: just as the home has historically been protected as a private domain, one's mental space should be off-limits to unjustified government intrusion. Legal scholars advocate updating search-and-seizure principles (such as the requirement of a warrant and probable cause) to explicitly encompass neurotechnological searches. Some have even suggested that compelled brain scans or mind-monitoring should be unreasonable: a violation of a fundamental mental privacy right that the Fourth Amendment can be interpreted to secure.[26]

However, applying the Fourth Amendment to BCIs raises difficult questions, and not all analyses are optimistic that current doctrine is sufficient. One issue is the third-party doctrine, which holds that information voluntarily shared with a third party is not protected by the Fourth Amendment's warrant requirement. Many BCI systems may rely on cloud platforms or external companies to process neural data. If a BCI user's brain data is stored on a company server, does the user lose their reasonable expectation of privacy in it? Roth confronts this question, terming government access to neural data "neurosearches."[27] He argues that if courts do not recognise neurodata as a special category, much of it could indeed fall under the third-party doctrine, meaning the government could subpoena or collect one's BCI data from a

[21]Ibid.
[22]See Myrick (2024).
[23]See Unger (2023a).
[24]See Unger (2023b).
[25]Ibid.
[26]See Kilbride and Iuliano (2015).
[27]See Roth (2024).

tech company without a warrant. In fact, the note concludes that under prevailing doctrine, compulsory brain-data searches might be deemed reasonable, so long as they meet basic Fourth Amendment standards, and that "commercial brain data falls within the third–party doctrine." This conclusion highlights a potential gap: extremely intimate data about one's mind could be treated legally the same as phone records or ISP data unless courts carve out an exception. Overall, there is a developing consensus in the literature that new safeguards are needed for "neuroprivacy." Proposals range from legislatively created "neurorights" to judicial recognition that brain data is categorically private.[28] Fourth Amendment scholarship on BCIs is thus grappling with how to ensure that the law keeps pace with technology, so that the privacy of our thoughts remains protected against unwarranted government scrutiny.

Fifth Amendment: Self-Incrimination and Neural Evidence

BCIs and related neurotech also provoke difficult questions under the Fifth Amendment's Self-Incrimination Clause, which protects individuals from being compelled to testify against themselves in criminal cases. The core issue is whether forcing someone to submit to a BCI-based interrogation or to surrender neural data would amount to compelling testimonial evidence. The Fifth Amendment privilege generally covers communications or revelations from a suspect's mind (like spoken words or written statements), but not physical evidence (like fingerprints, DNA, or a blood sample). Nonetheless, academic commentary reveals deep concerns that neurotech could be used to compel individuals to incriminate themselves through their brain activity. For example, Farahany examined emerging lie-detection technologies and argued that the Fifth Amendment would likely not prevent the government from accessing brain-based information unless courts expand the definition of what counts as testimonial evidence.[29] More recent scholarship is divided: some authors maintain that neurally decoded information is inherently testimonial (since it reveals the contents of one's mind), and thus forcing someone to undergo a brain scan or BCI test would violate the Fifth Amendment.[30] They point out that the essence of the privilege is to avoid "the cruelty of forced extraction" of information from the accused's lips or mind. Requiring a defendant to wear a BCI device that divulges their memories or thoughts could be seen as tantamount to interrogation without consent, effectively making them a "witness against themselves" via their brain signals. Other commentators note, however, that courts might view at least some neurodata as analogous to physical, non-testimonial evidence similar to how a court can compel a suspect to provide a fingerprint or appear in a lineup.[31] For instance, a brain-response indicating recognition of a face (a technique known as "brain fingerprinting") could be characterised as a physiological reaction, not a direct verbal confession. Given these ambiguities, some scholars have suggested shifting focus away from the Fifth Amendment to other doctrines: one proposal is that any compelled brain scan is a violation of the Fourth Amendment due to the invasive breach of mental privacy, obviating the need to classify the result as testimonial or

[28]See Ienca (2021).
[29]See Farahany (2012).
[30]See Roth (2024).
[31]See Kilbride and Iuliano (2015).

not. In summary, the literature underscores that BCIs blur the line between physical evidence and testimonial communication. There is a growing call for courts to treat neural data as deeply personal and potentially communicative, erring on the side of protecting individuals from being forced to divulge their thoughts. Until the law is clarified, the idea of compulsive neurotech examinations sits uneasily with the Fifth Amendment's guarantee that the government cannot simply mine a defendant's mind for incriminating evidence.

Methodology

The aim of this paper is to examine the constitutional implications of emerging BCI technologies through the context of U.S. case law, focusing on how these systems challenge existing interpretations of the First, Fourth, and Fifth Amendments. The paper will evaluate how the unique characteristics of neurodata interact with established legal protections related to free speech and thought, protection against unreasonable search and seizure, and the right against self-incrimination. The paper further reviews proposed legal frameworks, including emerging "neurorights," and draws comparisons to existing privacy laws such as HIPAA.

The goal is to explore policy and legal recommendations that balance technological innovation with the need to preserve individual autonomy and mental privacy. This includes advocating for specific safeguards, both technological and legislative, that address the unprecedented legal challenges posed by BCIs.

Results

BCI Risks to Constitutional Rights: First Amendment

The ability to rapidly and wirelessly connect people's minds so they can communicate through thoughts alone promises to revolutionise human interaction. While BCIs offer significant benefits, they also pose risks to privacy and cognitive liberty, defined as the right to freedom over one's own mental processes, thoughts, and consciousness. As with other types of data storage and transmission, neurodata would be susceptible to the same vulnerabilities, including hacking, hijacking, data corruption in the storage unit, and deliberate deletion by an outside source. However, neurodata has unique characteristics that make it arguably even more vulnerable than other forms of data. Neurodata is likely to include deeply personal thoughts, emotions, cognitive states, and information connected to a person's conscience. This highly sensitive information is unlikely to be found with the same level of detail in other forms of communication, such as email, and its presence in neurodata makes its loss even more personally threatening than the loss of other types of data. The primary basis for individual rights for U.S. citizens remains the U.S. Constitution and its associated Amendments. While the existence of neurodata itself would not appear to violate any constitutional rights, the potential ability for the government

to access or tamper with an individual's neurodata without their knowledge risks violating at least three of the Amendments in the Bill of Rights.

The authors of the U.S. Constitution listed the First Amendment as the first among all the amendments because they believed it protected the most important individual rights, including freedom of speech. The Amendment states, "Congress shall make no law […] abridging the freedom of speech".[32] BCIs transmit data silently, which could be literally interpreted as not involving vocal transmission, and, thus, does not constitute speech. However, in the U.S. Supreme Court case of *Ashcroft vs. Free Speech Coalition*, Justice Anthony Kennedy opined the strong connection between speech and thought by stating that "the right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought."[33] Other legal scholars support this perspective, with constitutional law historian Jud Campbell noting that "freedom of thought is widely accepted as one of the most basic freedoms afforded by the Constitution".[34]

However, BCIs, like any technology, are susceptible to security breaches. This vulnerability raises the possibility that someone could access or modify another person's neurodata or that a third party could intercept brain-to-brain communications between two individuals. This raise concerns that others could be "eavesdropping" on a person's silent conversations or even tamper with their stored neurodata without their knowledge. In both cases, the individual's thoughts could be exposed, downloaded, or made public without consent, leading to serious privacy and security issues. While these security breaches are similar to emails being hacked or written correspondence being copied, the content of neurodata is such that it could include information so sensitive that an individual would never have chosen to put it into written form. The person whose neurodata is being violated might not even be aware that their thoughts were being accessed or recorded. In more extreme cases, fear of BCI intrusion could lead to people censoring their thoughts, compromising their mental freedom due to the fear of being discovered. This, at minimum, may stifle free thinking and could also lead to a more significant erosion in self-worth. Justice Thurgood Marshall in *Procunier vs Martinez* stated that: "To suppress expression is to reject the basic human desire for recognition and affront the individual's worth and dignity".[35] Although Marshall was referring to censorship of written expression, the same principle could very well apply to any self-censorship of thought due to security risks, with equally harmful effects.

BCI Risks to Constitutional Rights: Fourth Amendment

While it is a fundamental right for U.S. citizens to have freedom of thought, it is also critical that these thoughts, whether stored in the human mind or stored digitally as electronic data, be protected from unauthorised access. The U.S. Constitution's Fourth Amendment grants citizens "the right of people to be secure in their persons

[32]See U.S. Constitution amend I.
[33]See *Ashcroft v. Free Speech Coalition* (2002).
[34]See Campbell (2017).
[35]See *Procunier v. Martinez* (1974).

[…] against unreasonable search and seizures" by the government.[36] This Amendment ensures that individuals have the right to privacy from government intrusion. If the government seeks to breach this privacy, law enforcement must first obtain a warrant, supported by probable cause and explicitly describing the place to be searched and items to be seized, as established by *Coolidge vs New Hampshire*.[37] In exigent circumstances, such as when a crime is being committed, law enforcement can initiate a search without a warrant based on probable cause. However, a court must subsequently review this action to determine its legality.[38] If the search is unjustified, any evidence obtained would be inadmissible in court.

Since BCIs can collect and interpret neurodata, including an individual's thoughts, memories, and mental states, law enforcement or government agencies would need probable cause and a warrant to monitor or extract personal BCI data legally. Some scholars have pointed to the Supreme Court's recent decisions like *Carpenter v. United States*, which recognised privacy interests in cell phone location records, as a template for treating personal neurodata differently given its sensitivity.[39] Unauthorised monitoring or accessing neurodata would constitute an unreasonable search while downloading, storing, or forwarding such data would be an unreasonable seizure: acts some have termed "neurocrime".[40] Illegal search and seizure by the government or law enforcement could occur in various situations, such as when there is urgency and waiting for a warrant might result in the destruction of evidence or some immediate harm, ignorance of legal requirements, overzealousness in securing an arrest, abuse of power, or misunderstandings of the law.

Privacy is a fundamental right that allows individuals to control their personal information and decide who can access it. Unauthorised access to BCI neurodata by the government or other parties could inadvertently reveal vast amounts of sensitive personal information such as health history, trade secrets, and other confidential information. Furthermore, while the most likely threats would involve hacking into a person's thoughts or intercepting their communications to other BCIs, one can imagine a dystopian scenario where the government tracks an individual's moods and consciousness. Individuals might be concerned about whether sufficient privacy protections are in place. They may feel vulnerable and unsure if they would be able to even detect unauthorised searches of their neurodata when interacting with others who have BCIs. This uncertainty could lead to feelings of suspicion and, in extreme cases, even paranoia.

Physical search and seizure events are typically detectable because it is apparent when a property has been disturbed in search of evidence. However, search and seizure of data via BCI access, whether performed legally or illegally, might not be as easily detectable by the individual whose thoughts and memories are being compromised. If a physical search is conducted without proper protocol, the evidence obtained is not admissible in court. Search and seizure of neurodata, however, might not leave any trace, making it difficult to prove that it actually occurred. The

[36]See U.S. Constitution amend. IV.
[37]See *Coolidge v. New Hampshire* (1971).
[38]See Warnken (2010).
[39]See Unger (2023b).
[40]ee Ienca and Haselager (2016).

government could assert that information implicating a defendant was obtained from other sources, avoiding any admission of improper BCI access. They could use the mined neurodata to uncover additional evidence, allowing them to build a case without directly relying on the neurodata itself. In this scenario, the neurodata influences the investigation but is not used as direct evidence, allowing authorities to avoid scrutiny. In order to not infringe upon an individual's right to privacy, the author believes accessing another person's BCIs should be prohibited under nearly all circumstances.

Government agencies and law enforcement professionals provide the counter-argument that probable cause should override the right to privacy when sufficient objective evidence justifies a search and seizure without a warrant.[41] For example, the government already exercises this power to extract cell phone and GPS data from service providers during criminal investigations, and a similar argument could be made for BCI-transmitted neurodata.[42] Authorities might claim that accessing neurodata is necessary for national security and public safety. The PATRIOT Act, enacted after the September 11, 2001, terrorist attacks, expanded the government's ability to search electronic data.[43] Article II of the PATRIOT Act permits government officials to obtain an individual's data from third-party sources, such as internet service providers, through which the data passes.[44] It also blurred the lines between collecting electronic data on foreign terrorists and domestic criminals, enabling surveillance of U.S. citizens under the pretext of monitoring foreign threats.[45] Therefore, current U.S. Department of Homeland Security powers could allow the U.S. government to access neurodata stored through BCIs in the future under the argument that it is necessary for the safety of U.S. citizens.[46] All types of data would be subject to this government authority, and presumably, BCI neurodata would be no different. This demonstrates that there is a limit to the absolute right to privacy from government intrusion. Utmost caution must be exercised when allowing this exception, however, and any authorised access of another's BCI neurodata should be rare and reserved for only the most exceptional circumstances.

BCI Risks to Constitutional Rights: Fifth Amendment

Laws against self-incrimination were designed to protect the accused from being compelled to provide information that could harm their defence. The Fifth Amendment of the U.S. Constitution states that "No person […] shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law".[47] This amendment safeguards the rights of those criminally accused and ensures a fair trial.[48] Justice William O. Douglas in *Ullmann vs The United States* stated, "The Fifth Amendment was designed to

[41]See Haddad (1977).
[42]See Gershowitz (2009).
[43]See Ahn (2014).
[44]See Ebenger (2008).
[45]See Buchhandler-Raphael (2012).
[46]See Delaney (2020).
[47]See U.S. Constitution amend. V.
[48]See Brilmayer and Norchi (1992).

protect the accused against infamy as well as against prosecution".[49] Rooted in English common law, the Fifth Amendment protects individuals from being forced--under duress or torture by police or other agencies--to provide information that could be used against them in court; the state must build its case using evidence not obtained by the defendant.[50]

While it may be straightforward for an individual to avoid verbally incriminating themselves by refusing to answer questions and thereby "take the Fifth," the ability of the government to search a person's neurodata could unintentionally reveal evidence related to the case, circumventing the need for voluntary disclosure and leading to an indirect form of self-incrimination. It also may be difficult, if not impossible, to mentally suppress information related to a crime in the mind and thoughts of the individual in question and, therefore, preclude discovery via a data search.[51] Moreover, a neurodata search may not leave any trace, so the individual might never know it occurred. Once self-incriminating data is obtained through BCI searches, it may be significantly easier for the state to build a case against a particular person, and the defendant may have no way of knowing if the state's case was, in part, built through accessing neurodata if the data was obtained surreptitiously. While data obtained through obviously illegal means would be inadmissible in court, one of the primary challenges with neurodata lies in tracing how it was acquired. As a result, information from neurodata might be used against a defendant under the pretence that it was obtained through other means. Legal scholars have debated whether a person's recorded neural signals – which might reveal, say, recognition of a crime scene or knowledge of a fact – should be considered an extension of their testimony (and thus protected) or treated as a physical trace akin to a fingerprint.[52] So far, no U.S. court has squarely decided this question in the context of modern neurotechnology.

Discussion

As BCIs become more prevalent and the risk of unauthorised access to neurodata increases, it is critical to develop robust measures to protect individual rights. The first step would be to incorporate safeguards into the BCI technology itself. Hardware designs that would prohibit hacking, at least to the greatest extent possible, should be mandatory if BCIs were to be widely accepted. The BCI software that manages data transmission must also be engineered to block unauthorised access and to provide the user alerts and notifications whenever their data is transmitted or accessed. Additionally, individuals should have the option to turn off data transmission at will and delete their own neurodata. Encryption should be implemented to prevent outsiders from permanently modifying or deleting an individual's neurodata.

Beyond technological safeguards, new laws must be developed to address the specific challenges BCIs pose. In order to protect the three rights discussed, legislation should make it illegal to access another person's BCI without their explicit consent,

[49]See *Ullmann v. United States* (1956).
[50]See Levy (1969).
[51]See Gherman and Zander (n.d.).
[52]See Kilbride and Iuliano (2015).

except in extremely limited circumstances. Furthermore, laws should be enacted to ensure that any evidence, direct or indirect, obtained through neurodata hacking would be inadmissible in court. Given the sensitivity of neurodata information, new laws that specifically apply to neurodata should be considered. Just as the Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 to protect all individuals' sensitive personal healthcare information, a potentially unique set of regulations should be established for neurodata. This would institute stringent data security standards commensurate with the level of sensitivity of the neurodata in regard to its storage, processing, and transmission.

In addition to data storage security, mechanisms that track the origin and transmission of neurodata would help protect the rights discussed above. Although it may be challenging to determine whether data was obtained with or without consent, future technology could enable the tagging or digital labelling of neurodata to identify its source.[53] Theoretically, each owner would have a unique digital label, making it apparent if specific neurodata was obtained from them. Once this technology is developed, laws could be enacted to specifically protect digitally labelled neurodata from being accessed, transferred, or stored without the owner's consent.

Conclusion

As brain-computer interfaces continue to develop rapidly, the technology holds transformative potential for the future and will fundamentally change how humans communicate. However, the emergence of BCIs also presents significant challenges in balancing technological advancement with protecting fundamental rights. In order to safeguard individual privacy rights, it will be essential to impose restrictions on the features and functionality of BCIs and to introduce additions to the current legal code to prevent misuse of neurodata by governments and other entities. The generation of this new unprecedented class of data will require careful examination of how to ensure privacy best when our most personal, innermost thoughts are recorded and potentially accessed by others. There is no longer an absolute guarantee of complete privacy, even within our own minds, in this future world with BCIs. Thus, not only is thoughtful legal regulation required for privacy protection, but the ethical consequences of the existence of neurodata should also be considered, such as issues of autonomy, discrimination, and self-identity. In addition to instantaneous thought communication between individuals, experts predict that BCIs will likely enable additional augmented cognitive capabilities such as enhanced learning, increased creativity, and the ability to move objects with our minds. These novel human enhancements will each create additional uncharted legal and ethical challenges as society navigates how to responsibly use the powerful, innovative benefits of BCIs while protecting basic fundamental rights to which all individuals are entitled.

[53]See Sirota (2023).

Bibliography

Ahn, J. (2014). *Seizure of Electronic Data under the USA PATRIOT Act Seizure of Electronic Data under the USA PATRIOT Act*. https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1434&context=student_scholarship

Akhavan, M. (2023). Possible risks in using brain-computer interfaces Open.mit.edu. https://open.mit.edu/c/teachremote/57f/possible-risks-in-using-braincomputer-interfaces

Allison, B.Z., Wolpaw, E.W. & J.R. Wolpaw (2007). Brain–computer interface systems: progress and prospects. *Expert Review of Medical Devices* 4(4):463–474. https://doi.org/10.1586/17434440.4.4.463

Bai, Z., Fong, K.N.K., Zhang, J.J., Chan, J. & K.H. Ting (2020). 'Immediate and long-term effects of BCI-based rehabilitation of the upper extremity after stroke: a systematic review and meta-analysis' in *Journal of Neuroengineering and Rehabilitation* 17(1):57. https://doi.org/10.1186/s12984-020-00686-2

Brilmayer, L. & C. Norchi (1992). 'Federal Extraterritoriality and Fifth Amendment Due Process' in *Harvard Law Review* 105(6):1217. https://doi.org/10.2307/1341728

Bublitz, C., Wolkenstein, A., Jox, R.J. & O. Friedrich (2019). 'Legal liabilities of BCI-users: Responsibility gaps at the intersection of mind and machine?' in *International Journal of Law and Psychiatry*. https://doi:10.1016/j.ijlp.2018.10.002

Buchhandler-Raphael, M. (2012). 'What's Terrorism Got to Do With It? The Perils of Prosecutorial Misuse of Terrorism Offenses' in *Florida State University Law Review* 39(4).

Burwell, S., Sample, M. & E. Racine (2017). Ethical Aspects of Brain Computer Interfaces: A Scoping Review. *BMC Med Ethics*. https://doi.org/10.1186/s12910-017-0220-y

Campbell, J. (2017). Natural Rights and the First Amendment [Review of *Natural Rights and the First Amendment*]. *The Yale Journal*, 127(2):246–489. https://www.Yalelawjournal.org/article/natural-rights-and-the-first-amendment

Delaney, K. (2020). 'The USA Patriot Act and Privacy: A New Frontier of Mass Surveillance' in *GPSolo*, 37(5):34–37. https://www.jstor.org/stable/27044798

Eastin, M.S., Brinson, N.H., Doorey, A. & G. Wilcox (2016). 'Living in a big data world: Predicting mobile commerce activity through privacy concerns' in *Computers in Human Behavior* 58:214–220. https://doi.org/10.1016/j.chb.2015.12.050

Ebenger, T. (2008). 'The USA PATRIOT Act: Implications for Private E-Mail' in *Journal of Information Technology & Politics* 4(4):47–64. https://doi.org/10.1080/19331680801978759

Edelman, B.J., Zhang, S., Schalk, G., Bunner, P., Muller-Putz, G. Guan, C. & H. Be (2025) Non-Invasive Brain-Computer Interfaces: State of the Art and Trends. *IEEE Rev Biomed Eng*. 18:26-49.

Farahany, N.A. (2012). 'Incriminating Thoughts' in *Stanford Law Review* 64:351-408.

George, D. (2020). 'Brain-Computer Interfaces and the Right to Cognitive Liberty' in *Washington Journal of Law, Technology, and Arts.* https://wjlta.com/2020/04/29/brain-computer-interfaces-and-the-right-to-cognitive-liberty/

Gershowitz, A.M. (2009). 'Searching Cell Phones Incident to Arrest: Can Courts and Legislatures Impose Limits on a Bright Line Rule?' Faculty Publications. https://scholarship.law.wm.edu/facpubs/1510

Gherman, D.E. & T. Zander (n.d.). *An ethical perspective on Passive BCI: Can we detect information from the human mind that is intended to be hidden?* https://neuroerg on omicsconference.um.ifi.lmu.de/wp-content/uploads/submissions/186.pdf

Goering, S., Klein, E., Specker Sullian, L., Wexler, A., Agüera, Y.A.B., Bi, G. Camena, J.M., Fins. J.J., Friesen, P., Gallant, J., Huggina, J.E., Kellmever, P., Marbelstonw, A., Mitechell. Ch., Parens. E. Pham, M., Rubel, A., Sadato, N., Teicher. M., Wassernan, D., Whittaker,

M., Wolpaw, J. & R. Yust (2021). Recommendations for Responsible Development and Application of Neurotechnologies. *Neuroethics* 14(3):365–386.

Green, R.A. (2021). 'Possibilities in bioelectronics: Super humans or science fiction?' in *APL Bioengineering*, 5(4). https://doi.org/10.1063/5.0079530

Haddad, J. B. (1977). 'Well-Delineated Exceptions, Claims of Sham, and Fourfold' in *The Journal of Criminal Law and Criminology (1973-)*, 68(2), 198. https://doi.org/10.2307/1142846

Ian (2024). Elon Musk's Neuralink and the Future of Human Enhancement Review of Elon Musk's Neuralink and the Future of Human Enhancement. Pressfarm. https://press.farm/elon-musks-neuralink-future-of-human-enhancement/

Ienca, M. (2021). On Neurorights. *Front Hum Neurosci*. 15. https://doi.org/10.3389/fnhum.2021.701258

Ienca, M. & P. Haselager (2016). 'Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity' in *Ethics and Information Technology* 18(2):117–129. https://doi.org/10.1007/s10676-016-9398-9

Rodrigues J.J.P.C., de la Torre, I., Fernández, G. & López-Coronado, M. (2013). 'Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems' in *Journal of Medical Internet Research* 15(8). https://doi.org/10.2196/jmir.2494

Kawala-Sterniuk, A., Browarska, N., Al-Bakri, A., Pelc, M., Zygarlicki, J., Sidikova, M., Martinek, R. & E.J. Gorzelanczyk (2021). 'Summary of over Fifty Years with Brain-Computer Interfaces—A Review' in *Brain Sciences* 11(1):43. https://doi.org/10.3390/brainsci11010043

Kilbride, M. & J. Iuliano (2015). 'Neuro Lie Detection and Mental Privacy' in *Maryland Law Review* 75(1): 163-193.

King, B.J., Read, G.J.M. & P.M. Salmon (2022). 'The Risks Associated with the Use of Brain-Computer Interfaces: A Systematic Review' in *International Journal of Human– Computer Interaction* 40(2): 131–148. https://doi.org/10.1080/10447318.2022.2111041

Levy, L.W. (1969). 'The Right Against Self-Incrimination: History and Judicial History in *Political Science Quarterly* 84(1):1-29. https://doi.org/10.2307/2147044

Liang, J., Stocco, A., Losey D.M., Abernethy, J., Prat, C.S. & R.N.P. Rao (2019) BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains. *Scientific Reports 16:9(1);*6115. doi: 10.1038/s41598-019-41895-7.

Mitrasinovic, S., Brown, A.P.Y., Schaefer, A.T., Chang, S.D. & G. Appelboom (2018). 'Silicon Valley new focus on brain computer interface: hype or hope for new applications?' in *F1000Res. 2018*;7;1327. https://doi.org/10.12688/f1000research.15726.1

Mullangi, S., Pollak, J.P. & S. Ibrahim (2019). 'Harnessing Digital Information to Improve Population Health' in *Harvard Business Review*. https://hbr.org/2019/05/harnessing-digital-information-to-improvepopulation-health

Mura, M.T.D. (2024). *Brain Computer Interface: the next big thing in motor and language rehab*. Tech4Future. https://tech4future.info/en/brain-computer-interface-rehab-2024/

Myrick, D. (2024). Cognitive Utopia or Dystopia? Brain-Computer Interface Enhancement and the Technological Singularity. *Oxford Political Review 2 April 2024.*

Nijboer, F., Clausen, J., Allison, B.Z. & P. Haselager (2011). 'The Asilomar Survey: Stakeholders' Opinions on Ethical Issues Related to Brain-Computer Interfacing' in *Neuroethics* 6(3):541–578. https://doi.org/10.1007/s12152-011-9132-6

Peterson, V., Galván, C., Hernández, H. & R. Spies (2020). 'A feasibility study of a complete low- cost consumer-grade brain-computer interface system' in *Heliyon*. 6(3). https://doi.org/10.1016/j.heliyon.2020.e03425

Roth, J.A. (2024). 'Neurosearches Note' in *Cornell Law Review* 109:997-1018.

Shahzad, A., Lee, Y.S., Lee, M., Kim, Y.G. & N. Xiong (2018). 'Real-Time Cloud-Based Health Tracking and Monitoring System in Designed Boundary for Cardiology Patients' in *Journal of Sensors* 1–15. https://doi.org/10.1155/2018/3202787

Sirota, D. (2023). *Unified tagging and labeling for structured and unstructured data*. BigID. https://bigid.com/blog/unified-tagging-and-labeling-for-structured-and-unstructured-data/

Unger, W. (2023a) 'Stay Out of My Head: Neurodata, Privacy, and the First Amendment' in *Washington and Lee Law Review* 80(4):1439-1521.

Unger, W. (2023b). ''The Constitutionality of Brain Searches' in *Hastings Constitutional Law Quarterly* 50(4):321-348.

U.S. Government Accountability Office (2022). *Science & Tech Spotlight: Brain-Computer Interfaces*. www.gao.gov.

Veena, N. & N. Anitha (2020). 'A Review of Non-invasive BCI Devices' in *Int. J. Biomedical Engineering and Technology* 34(3):205-223.

Vidal, J.J. (1973). 'Toward Direct Brain-Computer Communication' in *Annual Review of Biophysics and Bioengineering* 2(1):157–180. https://doi.org/10.1146/annurev.bb.02.060173.001105

Warnken, B.L. (2010). 'Four Ways to Make Valid Fourth Amendment Intrusions into Houses: Search Warrant, Arrest Warrant, Exigency, & Consent' in *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1567623

Warwick, K. (2020). 'Superhuman Enhancements via Implants: Beyond the Human Mind' in *Philosophies* 5(3):14. https://doi.org/10.3390/philosophies5030014

Zheng, H. (2025) Brain-Computer Interfaces: A Comprehensive Review of Technologies, Applications, and Challenges. *IJHSR.*

Cases

Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
Coolidge v. New Hampshire, 403 U.S. 443 (1971).
Procunier v. Martinez, 416 U.S. 396 (1974).
Ullmann v. United States, 350 U.S. 422 (1956).