

Ethical Frontiers: Navigating the Intersection of Neurotechnology and Cybersecurity

Er. Kritika^{1,*}

¹CSE, Independent Researcher, New Delhi, India

*Correspondence should be addressed to Er. Kritika, kritikaa2297@yahoo.com

Received date: September 27, 2024, **Accepted date:** December 04, 2024

Citation: Kritika Er. Ethical Frontiers: Navigating the Intersection of Neurotechnology and Cybersecurity. J Exp Neurol. 2025;6(1):21-25.

Copyright: © 2025 Kritika Er, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Keywords: Cybersecurity, Neurotechnology, Behavioural Neuroscience, Brain Computer Imaging, Privacy Concerns, Cognitive Enhancement

Commentary

Technological advances of neuroscience and cybersecurity have created a rapidly developing field and newer opportunities alongside challenges of ethics. Some of the emerging ideas that include, brain computer interfaces (BCIs), neuroimaging technologies (EEG, fMRI) etc., cognitive biometrics have produced fresh solutions to enhance cybersecurity, privacy, autonomy and data protection. Neuroscience is already changing at a very fast pace in the cyber security field. The prospect of using brainwave-based authentication and cognitive biometrics is vast, a far superior way to traditional processes of identification such as passwords or fingerprints [1]. Research has further shown that BCIs can be incorporated into access control systems to allow a BCIs-security mapping relationship [2]. Detecting stress or threat intent could then be incorporated into cybersecurity systems to further prevent insider threats as the system analyses the neural signals [3]. But the concern for security using the brain data presents few ethical questions. Neural data is associated with the disclosure of a person's emotional, cognitive, and even behavioral states. The storage and use of such data without informed consent and protection measures give rise to violations of people's privacy and abuse [4].

Ethical Dilemmas and Privacy Concerns

The ethical issues that arise from the integration consists mainly of privacy concerns and consent, as well as the manipulability of neural data [5]. Given the fast pace at which

neurotechnology is being developed and the fact that it is already being incorporated in security systems, concerns the management of cognitive privacy. Neural data, garnered through EEG, fMRI, or BCIs [6] is qualitatively different as it is deeper and more sensitive in contrast to the neural data that can reveal some of the patient's thinking process, feelings, plans, and even illnesses. This, in turn, raises very serious privacy issues since brain signals are an interaction of a person's thoughts and processes occurring in their head [7]. For instance, the data consistently generated by a man's brainwaves theoretically can be used to identify his emotional status and his levels of stress while investigating a security breach which violates the psychological sphere of human existence – thinking, can be monitored without the direct and acknowledged consent of the individual involved, a point that in itself could be abused to invasive monitoring or coercion [8,9] posing a very important ethereal issue on self-determination basing on an individuals' desire, consent and the consequent use of brain data for purposes other than security [10].

This principle of informed consent [11] is vital in medical practice, psychology, research, and any conduct deemed ethical. Neural data is an intricate subject, with individuals often not fully understanding the implications of sharing their brain activity data, making it difficult for the researchers to explain the dangers of its accumulation and analysis [12]. Informed consent requires individuals to be aware of how their data will be used, stored, and potentially shared. Data-mining and patterns from neural signals are possible, making it difficult to determine how much of it can be read from their brain. A basic neuroimaging [13] scan can elicit data about an individual's future mental stability, affective susceptibilities, and cognitive proclivities, making it even more challenging

to give informed consent [4]. A new ethical consideration is the reusability of neural data, as contexts like brain waves and other key neural signals may change over time due to changes in mood, health, or the environment [14]. This dynamic nature raises questions about the persistence of learning from neural data and whether individuals should be able to withdraw consent and stop using their data after certain time periods or states.

Data sovereignty is integral in discussion of privacy because people own their data such as fingerprints or retinal scan that are easier to be stored and protected as compared to other forms of biometric data [15]. Yet, there are emergent challenges to do with ownership, access, and sharing that come with neural data. The following questions are not given an answer in the current cybersecurity and privacy frameworks: the identity of the person whose brain activity was captured and recorded, and the respective organization which ensnared the data. CNN has established that neuronal data ownership is connected with data protection as well as storage [16] because violations or improper use could lead to disastrous outcomes affecting a person. It can be easily hacked with neural profiles within the reach of hackers and which can be used to perform identity theft or to manipulate individuals. Since there are no legal measures protecting data, ethical rules may not be sufficient to prevent the sale or sharing of gathered neural data, the violation of a person's right to cognitive privacy [17].

Real-time monitoring of the neural data through neuro-surveillance [3] also poses ethical issues in neuro-cybersecurity which could be utilized for tracking general states of cognition including stress, fatigue, and emotional state on high security work environment for instance to identify staff pressure or actions against organizational objectives. Because the brain activity is subjective and depends on external factors, there are questions about justice, as well as to the rights and equality in society. What is and what is not acceptable in terms of security interests and mental privacy is not clear, and given the development of neuro-surveillance technologies, this may become not very clear [18].

Neurotechnology is considered as the rising ethical issue because of the tendencies towards manipulations and coercion [19]. Cybercriminals can take advantage of neural weaknesses and make the targets make choices out of stimulating feelings of fear, trust or confusion. With neural data being considered relevant in the security practices, cognitive privacy, informed consent and data sovereignty issues should be addressed. Without such protective measures in place, the ordinary person has to face real threats of abuse, manipulation, and exerting coercion [20].

To understand the implications of the above ethical concerns, we need to look at case studies that are likely to arise in next-generation neurotechnology cyber-security risk. These are not

problems that will be found only in one system because these are defects which exist in many systems; more importantly, these points raise general concern over ethical problems that should receive more and better attention to safety and effective regulation.

Case Studies

Brainjacking and the vulnerabilities of BCIs

Brainjacking is defined as unauthorized control over brain implants or neurostimulators. Although the issue has been highlighted because of Risks in Brain Computer Interface (BCI) and other neural gadgets [21,22]. Another case study that was conducted in 2021 showed that rogue actors are capable of modifying a motor function, emotions, functional cognition or otherwise take control of a BCIs that was implanted in a patient [23]. This is a type of cyberattack that permits the attacker to manipulate neural signals so as to cause undesirable movements, thoughts, or dysphoria. Another interesting example was with deep brain stimulation (DBS) for Parkinson's disease, where hackers could alter the signals to the brain and result in movements that the patient does not want or even flee the device. The effects of brainjacking are not confined to any medical devices only but any BCIs that are used for optimizing cognition including military or high-security applications. This is on the backdrop of the highly increasing importance of strong cybersecurity protections around neurotechnological systems.

Unauthorized neural data access

Researchers from the University of Michigan and Johns Hopkins demonstrated potential security vulnerabilities in BCI systems that could expose neural signals during transmission [24,25], their analysis being a research-grade BCIs revealed multiple attack vectors affecting data integrity and participant privacy [26]. A data breach in 2022 at a neuroimaging technology firm leaked nearly 5,000 individuals' neural data including their cognitive and emotional patterns. The company relied on the EEG data to create the cognitive biometric authentication system, but a lot of the data was left unencrypted, and the company did not have sufficient security measures to prevent hackers from getting access to this data [27]. This breach led to ethical questions concerning the ownership and protection of neural information, for neural data contained detailed information about a person's cognitive condition, stress state, emotional susceptibilities, and mental disorders. It can be utilized for negative uses such as blackmail, identity theft or even use in psychological warfare. The occurrence also stirred discussions on the liability of organizations that work with delicate information, since its loss was a severe infringement on individual privacy. This case strengthens the call for more rigid legal frameworks concerning the storage, access and utilization of neural data in a business and security trade [28].

Neuro-surveillance in the workplace

Neuro-surveillance, which is the constant monitoring of the brain, is gradually becoming popular in such demanding careers as the financial market, police, and cyber security. This is where neuro-surveillance technologies were used in a financial firm in 2023 to observe employee stress during trading [29]. To monitor exhaustion, the firm was using wearable EEG devices to record continuous brain activity [30] and look for signs of cognitive overload or presumably emotional distress [31]. But this raised ethical dilemmas because the employees perceived that their mental privacy was infringed and issues relating to the use of the brain data collected, in relation to the promotion, bonuses, and job security. They also expected that their mental states might be produced in performance reviews or disciplinary proceedings against them. This case indicates how new technologies [32] of neuro-surveillance can lead to the formation of structures of power relations in the employment relationship asking questions about autonomy, consent and fairness [33].

Cognitive manipulation in social engineering attacks

Neurotechnology as a technology implies that it can be exploited socially in launching-and-overthrowing maneuvers. A permutation of neurofeedback phishing [34] attack was conducted in which the attackers successfully tricked individuals into revealing sensitive data. The attackers employed discreet neural signals to elicit trust or confusion, thus, the target was more vulnerable. They targeted aspects of human cognition which were understood through neurotechnology, which raised the probability of success of their attempts at phishing. The targeted individuals stated that they sometimes felt trustful or bewildered during the assault and thus revealed the passwords or any other financial data [35]. This case also raises the ethical issues that neuro-technologies may be exploited for social engineering and shows that present protections are insufficient to guard against such threats. The creators of neurotech have to guarantee that the technology could not be adapted for unlawful objectives.

The ethical quandaries of cognitive enhancements

A cybersecurity firm introduced transcranial direct current stimulation (tDCS) devices¹ to enhance the cognitive performance of its security analysts. The devices [36] were designed to improve focus, decision-making, and problem-solving abilities, especially in high-pressure situations like responding to cyberattacks [32]. However, some employees expressed concerns about the ethical implications of cognitive enhancement in the workplace. They felt pressured to use the devices to keep up with colleagues, fearing that refusing would put them at a competitive disadvantage. The long-term effects of repeated brain stimulation and potential coercion in neurotechnology use also raised concerns [37]. This case

underscores the ethical challenges of cognitive enhancement in professional settings, including questions about autonomy, coercion, and fairness [38].

In addition to illustrating the technical threats or ethical issues surrounding the integration of neurotechnology with cybersecurity, these cases are useful for thinking about a range of other ethical questions as well, among them cognitive privacy, informed consent, and influenceability [39]. Thus, analyzing these real-life situations, one can introduce principles of these technologies and an acute necessity in consistent ethical principles to solve issues, connected with their application.

Neurotechnology is a threat to cognitive liberty because other individuals or groups can command or spy on the thoughts and choices of a subject [40]. This is rather worrisome especially when one has to think of neuro-hacking as spammers and other evils of the internet get more intelligent [41]. There is a great concern of informed consent and data sovereignty, people must have ownership over their neural data. The idea of introducing neuro-surveillance [42] into the working environment leads to a number of questions concerning the nature of workplace monitoring. Smart drugs, drugs that in some way make your brain work better than before is viable but so is the ethical problem associated with it. Employees are likely to engage in these technologies [26] out of necessity to fit into the prevailing technologies that are in the market hence the cross between volition and coercion [34].

This is especially important, and we are witnessing the integration of neurotechnology into cybersecurity require improved regulatory frameworks as well as governance structures. This is an area government and international organizations need to embark on to determine policies that will offer neural data and cognitive privacy [43]. The first 2021 neurorights [44] law of Chile regulates people's mental data and cognitive self-ownership. They have to be protected in international human rights law so that they do not suffer prejudice and are not violated [45]. Neuroscience and cybersecurity: new paradigms of cooperation and their deep ethical implications. As for technologies, BCIs and cognitive biometrics [46] increase the level of secure parameters, at the same time impinging on privacy, agency, and neuro tree-map self-governance. To avoid all these risks, then the abuse of data must be handled well by setting good ethical standards and standards that must be followed [47]. Cooperation between neuroscience and ethics, cybersecurity professionals, and policy makers should better govern those technologies. Neuro-cybersecurity [48] may be seen as a branch of studies, dealing with the future of technologic and cybernetic connection with responsibility concerning neuro-cybersecurity, intellect, economics [49] and behavior. The development of neurotechnology requires that all member states should adapt their legal instruments for the protection of individuals fundamental rights. Neurotechnology can

¹ <https://neuromodec.org/what-is-transcranial-direct-current-stimulation-tdcs/>

only be useful without violating this right of privacy and personal decision as long as it is regulated by law and ethical considerations are put in place [50].

References

- Maiseli B, Abdalla AT, Massawe LV, Mbise M, Mkocho K, Nassor NA, et al. Brain-computer interface: trend, challenges, and threats. *Brain Inform.* 2023 Aug 4;10(1):20.
- Sindhu B, Rani BK. Complementing Biometric Authentication System with Cognitive Skills. In *Microelectronics, Circuits and Systems: Select Proceedings of Micro2021*. 2023 Jun 27: 457-65.
- Kritika M. A comprehensive study on navigating neuroethics in Cyberspace. *AI and Ethics.* 2024 May 2:1-8.
- White T, Blok E, Calhoun VD. Data sharing and privacy issues in neuroimaging research: Opportunities, obstacles, challenges, and monsters under the bed. *Hum Brain Mapp.* 2022 Jan;43(1):278-91.
- Ienca M, Starke G. *Brains and Machines: Towards a unified Ethics of AI and Neuroscience.* Elsevier; 2024 May 24.
- Tan W, Lee EJ. Neuroimaging insights into breaches of consumer privacy: Unveiling implicit brain mechanisms. *Journal of Business Research.* 2024 Sep 1; 182:114815.
- Brown CM. Neurorights, Mental Privacy, and Mind Reading. *Neuroethics.* 2024 Jul;17(2):34
- Ienca M, Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sci Soc Policy.* 2017 Dec;13(1):5.
- Hurley ME, Sonig A, Herrington J, Storch EA, Lázaro-Muñoz G, Blumenthal-Barby J, et al. Ethical considerations for integrating multimodal computer perception and neurotechnology. *Front Hum Neurosci.* 2024 Feb 16; 18:1332451.
- Pereira AD. Ethical challenges in collecting and analysing biometric data. *Ethical challenges in collecting and analysing biometric data.* 2020:108-14.
- Burkhardt G, Boy F, Doneddu D, Hajli N. Privacy behaviour: A model for online informed consent. *Journal of business ethics.* 2023 Aug;186(1):237-55.
- Susser D, Cabrera LY. Brain data in context: Are new rights the way to mental and brain privacy?. *AJOB neuroscience.* 2024 Apr 2;15(2):122-33.
- Yen C, Lin CL, Chiang MC. Exploring the frontiers of neuroimaging: a review of recent advances in understanding brain functioning and disorders. *Life.* 2023 Jun 29;13(7):1472.
- Yuste R. Advocating for neurodata privacy and neurotechnology regulation. *Nature Protocols.* 2023 Oct;18(10):2869-75.
- Hayek M. Biometrics and Personal Data as a Security Concern in the 21st Century?
- Pawlicki M, Kozik R, Choraś M. A survey on neural networks for (cyber-) security and (cyber-) security of neural networks. *Neurocomputing.* 2022 Aug 21;500:1075-87.
- Rainey S, McGillivray K, Fothergill T, Maslen H, Stahl B, Bubltz C. Data and Consent Issues with Neural Recording Devices. *Clinical Neurotechnology meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications.* 2021:141-54.
- Kritika EM. Neuroethical Quandaries at the Crossroads of Cyberspace. *Scientific and Practical Cyber Security Journal.* 2024 Apr 12;8(1):57-63.
- Farina M, Lavazza A. The 'NeuroGate': neuromorphic intelligence, extended mind, and neurorights. *Synthese.* 2024 Nov 11;204(5):148.
- Privitera AJ, Du H. Educational neurotechnology: Where do we go from here?. *Trends in neuroscience and education.* 2022 Dec 1;29:100195.
- Bernal SL, Celdran AH, Maimo LF, Barros MT, Balasubramaniam S, Perez GM. Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. *Ieee Access.* 2020 Aug 17;8:152204-22.
- Angelakis D, Ventouras E, Kostopoulos S, Asvestas P. Cybersecurity Issues in Brain-Computer Interfaces: Analysis of Existing Bluetooth Vulnerabilities. *Digital Technologies Research and Applications.* 2024 Jul 10;3(2):115-39.
- Bernal SL, Celdrán AH, Pérez GM, Barros MT, Balasubramaniam S. Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges. *ACM Computing Surveys (CSUR).* 2021 Jan 2;54(1):1-35.
- Schalk G, Leuthardt EC. Brain-computer interfaces using electrocorticographic signals. *IEEE reviews in biomedical engineering.* 2011 Oct 17;4:140-54.
- Miller KJ, Hermes D, Staff NP. The current state of electrocorticography-based brain-computer interfaces. *Neurosurgical focus.* 2020 Jul 1;49(1):E2.
- Miyamoto K, Trudel N, Kamermans K, Lim MC, Lazari A, Verhagen L, Wittmann MK, Rushworth MFS. Identification and disruption of a neural mechanism for accumulating prospective metacognitive information prior to decision-making. *Neuron.* 2021 Apr 21;109(8):1396-408.e7.
- Levy R. Ethical risks of neuro-surveillance technologies. *Journal of Applied Philosophy.* 2022;39(2):120-35.
- Chatterjee H. Data sovereignty and brain privacy. *Ethics & International Affairs.* 2022;36(2):245-60.
- Vinck M, Uran C, Spyropoulos G, Onorato I, Broggin AC, Schneider M, et al. Principles of large-scale neural interactions. *Neuron.* 2023 Apr 5;111(7):987-1002.
- Dietrich BJ, Sands ML. Seeing racial avoidance on New York City streets. *Nat Hum Behav.* 2023 Aug;7(8):1275-81.
- Aydin M. Ethical implications of neuro-surveillance in the workplace. *Journal of Business Ethics.* 2023;130(4): 1031-45.

32. López-Silva P, Wajnerman-Paz A, Molnar-Gabor F. Neurotechnological Applications and the Protection of Mental Privacy: An Assessment of Risks. *Neuroethics*. 2024 Jul;17(2):31.
33. Illes J. Neuroethical considerations in cognitive liberty. *American Journal of Bioethics Neuroscience*. 2023;14(3): 285-97.
34. Park KW, Bu SJ, Cho SB. Evolutionary optimization of neuro-symbolic integration for phishing URL detection. In: *Hybrid Artificial Intelligent Systems: 16th International Conference, HAIS 2021, Bilbao, Spain, 2021 Sep; 22–24, 2021, Proceedings 16 2021* (pp. 88-100).
35. Thomopoulos GA, Lyras DP, Fidas CA. A systematic review and research challenges on phishing cyberattacks from an electroencephalography and gaze-based perspective. *Personal and Ubiquitous Computing*. 2024 Mar 19:1-22.
36. Chase HW, Boudewyn MA, Carter CS, Phillips ML. Transcranial direct current stimulation: a roadmap for research, from mechanism of action to clinical implementation. *Molecular psychiatry*. 2020 Feb;25(2):397-407.
37. Navarro MS, Dura-Bernal S. Human Rights Systems of Protection from Neurotechnologies that Alter Brain Activity. *Drexel L. Rev.* 2023;15:893.
38. Lavazza C. Brain hacking: Ethical challenges of cognitive biometrics. *Ethics and Information Technology*. 2023;25(2):201-10.
39. Kritika M. A comprehensive study on navigating neuroethics in Cyberspace. *AI and Ethics*. 2024 May 2:1-8.
40. Bernal SL, Celdrán AH, Pérez GM. Eight reasons why cybersecurity on novel generations of brain-computer interfaces must be prioritized. *arXiv preprint arXiv:2106.04968*. 2021 Jun 9.
41. Alexandre e Castro P. What Neurohacking Can Tell Us About the Mind: Cybercrime, Mind Upload and the Artificial Extended Mind. In: *Challenges of the Technological Mind: Between Philosophy and Technology*. Cham: Springer Nature; 2024 May 16. pp. 43-62.
42. Rickli JM, Ienca M. The security and military implications of neurotechnology and artificial intelligence. *Clinical Neurotechnology Meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications*. 2021:197-214.
43. Farahany NA. Neural data privacy: Challenges and solutions. *Frontiers in Neuroscience*. 2023;17.
44. Istace T. Neurorights: The debate about New Legal safeguards to protect the mind. *Issues Law Med*. 2022 Spring;37(1):95-114.
45. Terris C. Moving beyond context: Reassessing privacy rights in the neurotechnology era. *AJOB Neuroscience*. 2024 Apr 2;15(2):144-6.
46. Magee P, Ienca M, Farahany N. Beyond neural data: Cognitive biometrics and mental privacy. *Neuron*. 2024 Sep 25; 112(18):3017-28.
47. Balantrapu SS. Ethical Considerations in AI-Powered Cybersecurity. *International Machine Learning Journal and Computer Engineering*. 2022 Mar 24;5(5).
48. Liv N, Greenbaum D. Cyberneurosecurity. In: *Policy, Identity, and Neurotechnology: The Neuroethics of Brain-Computer Interfaces*. Cham: Springer International Publishing; 2023 Apr 27. pp. 233-51.
49. Kritika. A comprehensive study on the emerging role of neuroeconomics dynamics in cybersecurity. *Asian Journal of Interdisciplinary Research*. 2024;7(2):27-43.
50. Goering S, Klein E, Specker Sullivan L, Wexler A, Agüera y Arcas B, Bi G, et al. Recommendations for responsible development and application of neurotechnologies. *Neuroethics*. 2021 Dec;14(3):365-86.