

Hacking BCI Ethics

M. Welter¹, F. Lotte¹

¹Inria Center at the University of Bordeaux/LaBRI, Bordeaux, France

E-mail: marc.welter@inria.fr

ABSTRACT: In the age of surveillance capitalism, the exploitation of personal data has become ubiquitous. Although, this can be beneficial to personalize user experience, such data is also regularly exploited for manipulation and harm, e.g. to influence voting behaviour or even incite violence. As the emergence of Brain-Computer-Interface (BCI) technologies can grant unprecedented access to private and mental data, BCI users need to be protected against unethical exploits of their brain data. To be able to defend against attacks, it is helpful to be aware of possible attacks a priori. To this end, we propose to adopt an adversarial approach inspired by ethical hacking in cybersecurity to hack BCI ethics. By taking the hypothetical perspective of unethical actors, e.g. surveillance capitalists, we can determine concrete ethical vulnerabilities in BCI systems and work on patches to fix them.

INTRODUCTION

It has been suggested that consumer Brain-Computer-Interfaces (BCIs) that record and process data from their user's brain could soon be adopted by the general public.[1] At the same time, we live in an era of unprecedented and ubiquitous algorithmic data exploitation. In unison with (proto-)authoritarian governments, data appropriating businesses have created a new economy based on surveillance and the exploitation of personal user data.[2] In this economic model, often described as surveillance capitalism[3] or, more recently, technofeudalism[4], data collection and analysis algorithms are used to influence user behaviour, e.g. by personalizing advertisements in order to push product sales.

However, besides such relatively innocuous commercial goals, these algorithms are also used more and more in political contexts, e.g. to influence voting behaviour during political elections.[5] Although, data-driven algorithms have the potential to improve user experience through personalization or by offering access to online communities, it has been shown that, in practice, surveillance capitalist platforms tend to promote hateful and divisive messages by design and as such, pose an existential threat to democracy and social cohesion.[2] The danger posed by these algorithms (and their owners) becomes even more evident, if one considers the definition of 'the art of using technological tools to alter the cognition of human targets' as 'cognitive warfare', e.g. by NATO.[6] Taking this definition literally, one can argue that, given the omnipresence of technological surveil-

lance today, e.g. through smartphones, microphones and cameras, human cognition and thought are under constant assault from surveillance capitalists and governments. Indeed, the human brain has been called the 'battlefield of the 21st century'.[6]

For now, the weaponized surveillance algorithms used to influence human cognition, mostly rely on behavioural data, e.g. clicks and likes. However, in many cases it can remain challenging to infer cognitive and affective processes from non-physiological data. For example, we can consider the case of a person watching or listening continuously to video or audio streams on a digital platform. This person might be highly attentive and engaged towards the stimuli, but might not exhibit any overt behavioural correlates of their appreciation. Time spent is commonly used as a surrogate for engagement, however, this is highly flawed, because a stream can just be running without anyone watching/listening. Therefore, surveillance capitalists often implement automated pop-up windows after long viewing times, so that users need to engage with the platform (e.g. click on a button) from time to time and generate explicit feedback that is then used by the algorithms. In contrast, physiological computing could allow the implicit extraction of relevant mental states from the user without requiring explicit user feedback.[7]

Unsurprisingly, companies and governments have started to realize the potential of physiological computing and BCI which is evident in their increasing economic investments (estimated around \$33.2 billion in 2021 [8] regarding such technologies.[9])

Given the increasing popularization of wearable physiological computing devices that are often embedded in surveillance capitalist ecosystems, e.g. Apple's walled garden which already includes a patent application for wireless in-ear headsets with integrated EEG electrodes [10], it seems highly likely that in the near future (neuro-)physiological data will be commonly exploited by surveillance entities in order to fine-tune their algorithms for nefarious purposes. Therefore, ethical reflections on future use of physiological computing systems in general and BCIs in particular are critical in order to defend individual humans and democratic societies from the threats posed by surveillance capitalism.

To this end, we propose an adversarial approach inspired by ethical hacking in order to hack BCI ethics. Ethical hacking is a concept from cybersecurity where an agent

plays the role of an unethical adversary and tries to discover system vulnerabilities in order to be able to better protect the system against real attacks. Indeed, simulating attacks during authorized penetration testing of computer systems by ethical hackers has become a highly important technique to mitigate security risks. [11]

Analogous to ethical hacking in cybersecurity, we propose that adopting adversarial roles can be beneficial to mitigate ethical risks that arise from Neurotechnology. First, we will begin with a brief overview of the state-of-the-art of BCI ethics. Afterwards, we will describe the framework of hacker ethics that constitute the ethical foundation of this work. Then, we will define the general methodology of applying ethical hacking to BCI ethics. Next, we will illustrate our approach in a hypothetical case study by applying this method on a type of passive BCI that is currently developed and of particular interest to surveillance capitalists and authoritarian governments. After elaborating on the ethical risks posed by this BCI system, we will also discuss how these risks could be patched in order to protect its users.

ETHICAL BACKGROUND

BCI Ethics:

The emergence of BCI technology is accompanied with ethical risks concerning individual users and societies as a whole. Although, until now, the development of BCI ethics has been outpaced by its commercialization (Boonstra, 2025), the need for ethical reflection of BCI has been recognized (see [12] for a review on BCI ethics). Ethical issues in BCI concern concepts such as privacy [13], agency[14], inclusivity[15], among others.

Various techniques to identify and assess ethical risks arising from BCI technology have been developed (e.g. [13], [16]). Notably, Krol & Zander also proposed an adversarial approach to BCI ethics in which they call for the development of unethical BCI systems under controlled and ethical laboratory conditions.[1] While we believe that this proposal is promising and should be further explored, it suffers from two major limitations. First, this method does not allow to explore the potential ethical risks of technology that is not quite ready to be implemented yet. However, potential ethical risks should ideally be considered before a technology can be physically realized. Secondly, some BCI systems might be too unethical for researchers to get approval from an ethics committee and test them in laboratory conditions, e.g. if they are used for torture. In the following, we will present an alternative adversarial method inspired by ethical hacking to be used for ethical thought experiments regarding BCI.

Hacker Ethics:

Although, originally ‘hacker’ used to refer to creative tinkers in a more general way[17], it is nowadays more commonly used to describe actors that access or exploit computer systems unauthorized.[18]

On an individual scale, such actors can be malicious, e.g. so-called black hats[11], however, hacker culture in general is closely aligned with liberalism. Although, there is no unitary code of hacker ethics, liberal ideas, such as freedom, privacy, equal opportunity, meritocracy, etc., can be considered general moral commitments for many hackers.[19]

As such, hackers are in direct ideological opposition to surveillance capitalists and authoritarian governments.¹ Indeed, hackers and hacker organizations, such as the Chaos Computer Club in Germany² are some of the most prolific critics of surveillance capitalism and authoritarian governments.

This paper follows in the liberal tradition of hacker culture and its ethical values. Unfortunately, these values are currently under attack from surveillance capitalists in cahoots with authoritarian government.[3] In the next section, we will, thus, discuss how principles from ethical hacking can be used to defend these values and ourselves against this assault in BCI.

ETHICAL HACKING FOR BCI ETHICS

General Method:

This section describes the general method to hack BCI ethics. This method consists of the following steps that will be further described in the next paragraphs: 1. Designing a BCI system. 2. Embedding this system in a social context. 3. Adopting an adversarial role to find ethical exploits in this system. 4. Develop ethical patches for this system.

BCI System 1. Designing the System:

In order to hack BCI ethics, we first need a BCI system to hack. However, at least for now, few consumer BCI system that function reliably exist. As such, it remains challenging to truly hack BCIs currently.

Nonetheless, novel technologies emerge from existing economic and political systems, and as such, we can hypothesize how hypothetical BCIs could be maliciously exploited by unethical actors in these systems. Moreover, a plethora of science fiction media include fictional BCIs[21], and can be used as inspirational source in order to design hypothetical BCI systems to hack.

Although, this reliance on BCI thought experiments might seem like a limitation, flaws in a product should ideally be fixed before its public release. Therefore, it is important that we³ consider the ethical risks of BCI, before the technology becomes widely adopted with a high risk of unethical use.

Still, even hypothetical BCI systems need to be relatively realistic in order to be useful and should be neither logically nor physically (according to current scientific un-

¹Unsurprisingly, hackers are mostly portrayed negatively in mainstream media.[19]

²Not to be confounded with the Chaos Computer Club in France which was a false flag operation to survey hackers by security agencies.[20]

³Especially those of us who develop BCI.

derstanding) impossible. However, a BCI system does not necessarily need to work in order to be used unethically, e.g. as is the case with polygraphy-based lie detection in some countries, e.g. USA.[22]

2. Example: Given the worldwide loneliness epidemic and general disappointment with the current state of dating apps, we can imagine that a BCI dating system could be used to optimize romantic matches based on neural markers of interest, arousal, etc.

Embedding the BCI System 1. Technology in context:

Technology does not exist in a neutral void, but is always embedded in political and economic, and thus, ethical, contexts. Therefore, in order to be useful, our hypothetical BCI system also needs to be embedded in such contexts.

2. Example:

Given the increasing popularity of far-right politicians worldwide, we could, for example, imagine how a BCI system could be exploited in a (post-)fascist regime.

Adopting an Adversarial Role 1. Ethical Exploits:

Given a BCI system and a social context, we can then consider which unethical actors would want to use this BCI system and what their aims, e.g. political, economic, etc., are. Afterwards, one can adopt the role of such an unethical actor and consider how one would exploit the BCI system from their perspective. Here, we can also take inspiration from the ethical vulnerabilities of already existing technology. For example, although BCIs are still a very niche technology, smartwatches have become quite common and many of these devices record physiological data such as cardiac activity which can contain sensitive personal information.[23]

2. Example:

Given access to neural data and the ability to match potential romantic partners, we can imagine that a fascist regime could use neural data to identify neuro-divergent users for eugenic purposes.

Ethical Patches 1. Fixing ethical vulnerabilities:

As with computer vulnerabilities, discovered ethical vulnerabilities should also be patched. Unfortunately, patching ethical vulnerabilities can be even more complicated than patching software, because ethical exploits often concern societal systems as a whole. Still, similarly to ethical hackers in cybersecurity, we think that it is crucial to disclose the discovered vulnerabilities as a first step to develop patches. Only when one (and ideally, society as a whole) is aware that a flaw exists, can one start to fix it. As such, transparency, communication, regulation and education are often critical to patch ethical risks. Indeed, the various ethical patches proposed in this article are deeply intertwined. Transparent technologies permit educated users to better apply their critical reasoning skills, as well as vote for politicians proposing ethical laws and regulations (at least in liberal democracies).

2. Example:

Fixing ethical vulnerabilities in a fascist society can be more than complicated and pretty dangerous. From a liberal perspective, fascist societies are inherently unethical, as such we could imagine liberal hacktivists to engage in cyberattacks against such a BCI used for eugenics, e.g. by spoofing fake brain signals in order to confound its processing algorithms and protect the users.

After describing the general method to hack BCI ethics, we will now illustrate it with a case study.

Case Study:

BCI System In this case study, we will describe a hypothetical BCI system whose real-world adoption by consumers would come with severe ethical risks. As we already briefly mentioned in the introduction, passive BCIs could improve user experience by personalizing these experiences, e.g. by personalizing media or product presentation based on a user's neural states. This BCI would measure neural correlates of user engagement, e.g. attentional markers such as neural alpha activity, in order to decode a user's appreciation.[24] This BCI system would then function similar to a Like button, but without requiring explicit user behaviour and be used to train algorithms and make predictions.

Embedding the System in a socio-economic context

Given the current surveillance capitalist economic system in which data are precious commodities, we believe that such hypothetical like decoding BCI systems are probable to be developed in the near future. Therefore, we embed this hypothetical BCI in our current human state of affairs, i.e. we consider how such a technology could and likely would be unethically used if it would arise in our current world.

Adopting an adversarial role 1. Unethical Actors:

Various parties could profit from the unethical use of the hypothesized user experience decoding BCI system and the personal data it records. Potential bad actors range from petty criminals to organized crime, as well as companies and governments. Although, regular criminals could be interested in personal data collected by this BCI, e.g. in order to blackmail a victim for based on neural markers of sexual orientation, we believe that, in the current geopolitical context, surveillance capitalist companies and authoritarian governments pose deeper ethical risks, due to their scale and global power. In particular, surveillance capitalist and governments are typically funding, developing, providing and regulating new technologies and as such have some moral responsibility in their regards⁴. Therefore, we will focus on how these entities could exploit a user experience decoding BCI for their unethical purposes.

2. Hacking:

⁴As do researchers working on these technologies.

In this section, we will, now that we have adopted the role of unethical surveillance capitalist and governmental actors, elaborate on possible ethical vulnerabilities for these actors to exploit if our fictional user experience decoding BCI would exist already. Both types of actors are already heavily exploiting personal data for economic and political gains. Although, purely behavioural data can already be sufficiently informative for many purposes, physiological data from various sources, e.g. health records, fitness trackers, etc. are being more and more integrated in surveillance capitalist data pipelines.[25] As such, most of the ethical risks arising from user experience decoding BCIs are not completely new, but they complement and enhance the ethical risks that are already present in our contemporary world.

In the following, we will discuss a few specific ways how a user experience decoding BCI could be used by surveillance capitalists and unethical governments to manipulate and repress humans.⁵

a) Manipulation:

As mentioned in the introduction, personal data is used by surveillance capitalists and governments to influence human cognition and behavior through the algorithmic micro-targeting of individuals. We imagine that a user experience decoding BCI measuring neural correlates of personal likes and dislikes could improve micro-targeting, by optimizing how personalized stimuli presentation and messaging affects a user's brain. Next to capitalist interest of selling products to consumers, this BCI system could also be used for propaganda and political influence, e.g. by using its data in micro-targeting to affect the outcome in political elections. Furthermore, surveillance capitalist algorithms have been used to promote hate and violence, e.g. on Facebook in the case of the genocide in Myanmar[26], and we can imagine that access to neural data could be used to optimize the evoked negative emotions, e.g. dislike, and consequently, evoke even more violent behavior in the future.

b) Repression:

Besides manipulation, a user experience decoding BCI could also be used in repressing 'undesirable' humans and ideas. For example, neural responses evoked by stimuli featuring attractive persons of different genders can be informative about sexual orientation[27] which could then be used to optimize the existing repression of LGBTQ+ persons who in some countries still risk severe punishment, e.g. the death penalty. Moreover, brain activity evoked by political stimuli can similarly be informative about a user's political beliefs.[28] Such information could then be used by companies to repress activists or unions, or by authoritarian governments to repress political opposition. Nowadays, USA immigration is already checking immigrant social media and personal computing devices and negotiating access to biometric

data from EU citizens. As such, we can also imagine future immigration to include neural data collected from user experience decoding BCIs in their assessments.

Even more extremely, personal (meta-)data and surveillance capitalist technologies are already used in AI-assisted targeting to determine human targets in military contexts, e.g. currently by the IDF in Gaza.[29] Such targeting systems assign a numerical value to individuals, often based on all kinds of (mostly) correlational data and meta-data. Then, an arbitrary threshold is defined and each individual above this threshold is considered a legitimate military target by the system. It seems plausible that neural data would also be used by such systems. And that, for example in the context of the war in Gaza again, neural data relating to liking innocent objects, e.g. water melons which have been adopted a pro-Palestinian symbol, could increase one's correlational score determined by an AI-assisted targeting system. And therefore, the probability to be killed in a military attack.

Finally, we further hypothesize a user experience decoding BCI could be unethically used to personalize torture methods and optimize the amount of harm caused in the victim. Various art stimuli have been used for torture prisoners in the past, e.g. surreal art during the Spanish Civil War, or heavy metal music by the USA in Guantanamo Bay. As a working user experience decoding BCI could also decode negative user experience, e.g. dislike, the technology could be abused to optimize the stimuli presentation in order to cause the most suffering in the tortured victim.

Ethical Patches The first step to patch the ethical flaws discussed above, is to disclose their existence. Consumers in particular need to be made aware of the ethical issues of technology they use, so they can make an informed decision whether they want to use it or not. This is especially important, as both governments and companies increasingly implement opt-out instead of opt-in data sharing procedures which does not allow for informed consent, e.g. in the case of the highly vulnerable electronic health records in Germany or AI-training in Whatsapp respectively, and prey on the uninformed and disinterested.⁶ Instead, consumers need to be educated and informed about the power of technologies and how they are embedded in current power structures. Many BCI researchers work in academia and are educators as well. As such, the community is in a privileged position to promote critical reasoning skills in face of technological innovation. Furthermore, in order to truly understand technology, it can not be a black box. Therefore, data processing pipelines need to be transparent and interpretable, so that consumer know what is done with their personal data.

Finally, regulations and legal frameworks can be used to protect consumer rights (if they are enforced with enough deterrence effect), e.g. data ownership and pri-

⁵This is not meant to be an exhaustive list of all possible ethical exploits of this BCI system, and we encourage interested readers to themselves adopt an adversarial role and search for further ethical exploits that we have missed.

⁶Unsurprisingly, electronic health data is also planned to be easily and legally shareable with companies.

vacy in the case of passive BCI. Indeed, various governance frameworks for Neurotechnologies have been developed by regulatory and government organizations and researchers (see [30] for a scoping review). Notably, international bodies such as UNESCO[8] have developed ethical guidelines for neurotechnology. Furthermore, legal acts, such as the EU AI Act, are currently being adopted by governments in order to regulate AI systems, including BCI, and protect their users. Given the structural power imbalance between citizens and governments, as well as between consumer and companies, we believe that legal protection of consumers and civil rights is of utmost importance in order to protect individuals against unethical applications of BCI technology. Still, (over-) regulation of BCI could stifle urgent technological innovation, e.g. medical treatments, and as such, consensus on BCI governance remains inexistent.[30]

DISCUSSION

In this paper, we propose adopting the role of unethical actors for thought experiments in BCI ethics in order to defend against ethical exploits.

Although, we are aware that bad actors could potentially be inspired by our hypothetical examples and use them to exploit BCI systems in the real world, security by obscurity is generally not considered adequate protection.[31] In contrast, ethical hacking approaches have been widely embraced by the cybersecurity community in order to defend systems against malicious attacks. Similarly, we believe that concepts from ethical hacking in cybersecurity can be used to inform BCI ethics. By taking the perspective of unethical actors, e.g. surveillance capitalists, we can investigate how and for which purposes BCI technology could be exploited. This knowledge about potential ethical vulnerabilities can then be employed to develop safeguards for users and promote the development of ethical BCI systems. Therefore, BCI education and dissemination are crucial for consumers to be aware about its potential risks. As such, we can consider the existence of a moral duty for the BCI community to inform the public about potential benefits and risks of the technologies they develop. However, given the existing power structures in which technologies are embedded, knowledge alone might not be sufficient to protect their users. In these cases, legal protections need to be passed and enforced to discourage bad actors from exploiting a technology. However, as legislative bodies and surveillance capitalists often share common interests, e.g. the surveillance of consumers and citizens, the effectiveness of BCI regulations can be questionable. For example, although the EU AI Act grants some protection to consumers, many loopholes that could be exploited unethically remain.[32] Furthermore, the recently proposed EU Digital Omnibus closely aligns with big tech lobbyist positions and weakens some of the previously established legal protections and widens the allowed exploitation of personal data, including for AI training.[33]

Given that the main bad actors in surveillance capitalism are governments and powerful companies, it can seem hopeless to try and defend against the cognitive war they are conducting against us. However, not all is lost yet. For now, it is still possible to criticize unethical behaviour from both companies and governments and vote for politicians one considers ethical in elections (at least in most EU countries) which can result in laws one would consider ethical. For example, one can still have hope that large-scale activism has contributed towards the current rejection of the proposed EU chat control which would have severely weakened consumer cybersecurity under the guise of ‘child protection’ by EU parliament.[34] This suggests that political actions such as raising awareness through dissemination can still be used to protect against attacks on liberal values, such as privacy.

CONCLUSION

Given the potential public adoption of BCI in the near future, we are faced with potential existential ethical risks that threaten liberal values, democracy and even human lives. In a world where powerful actors have great financial and political interest to use BCI unethically and exploit user brain data for their own goals, e.g. manipulation and repression, it is crucial to determine how such actors could profit from such use, ideally before consumers get caught in exploitative structures, e.g. surveillance capitalist ecosystems. To this end, we proposed an ethical hacking approach towards BCI ethics which takes an adversarial perspective to discover ethical vulnerabilities in BCIs from the point of view of bad actors and patch these flaws.

REFERENCES

- [1] Krol LR, Zander TO. Create no evil? a call to cross ethical boundaries. In: 3rd Neuroergonomics Conference. 2021.
- [2] Dawson J. Who controls the code, controls the system: Algorithmically amplified bullshit, social inequality, and the ubiquitous surveillance of everyday life. *Sociological Forum*. 2023;38.
- [3] Zuboff S. *The age of surveillance capitalism* (. 2019).
- [4] Durand C. *Techno-féodalisme*. La Découverte: Paris (2020).
- [5] Trauthig I, Valenzuela S, Howard P. The role of generative ai use in 2024 elections worldwide. 2025.
- [6] Claverie B, Cluzel F du. *The cognitive warfare concept*. 2022.
- [7] Welter M, Bouneau A, Lotte F, Ward T. Towards curating personalized art exhibitions in virtual reality with multimodal electroencephalography-based brain-computer-interfaces. *Art & Perception*. 2023;11(2).
- [8] UNESCO. *The risks and challenges of neurotechnologies for human rights*. 2023.
- [9] Drinkall J. Capitalist telepathics, psychic debt and the search for collective intelligence. *TOPIA*. 2022;45.

- [10] Azemi E et al. Biosignal sensing device using dynamic selection of electrodes. US Patent Application Number: US 2023/0225659 A1. 2023.
- [11] Yaacoub JPA, Noura HN, Salman O, Chehab A. A survey on ethical hacking: Issues and challenges. 2021. arXiv: 2103.15072 [cs.CR]. [Online]. Available: <https://arxiv.org/abs/2103.15072>.
- [12] Lang A, Coin A, Dubljevic V. A scoping review of the academic literature on bci ethics. Apr. 2024.
- [13] Mecacci G, Haselager P. Identifying criteria for the evaluation of the implications of brain reading for mental privacy. *Science and Engineering Ethics*. 2019;25(2).
- [14] Haselager P. Did i do that? brain-computer interfacing and the sense of agency. *Minds and Machines*. 2013;23(3).
- [15] Livanis E, Voultsos P, Vadikolias K, Pantazakos P, Tsaroucha A. Understanding the ethical issues of brain-computer interfaces (bcis): A blessing or the beginning of a dystopian future? *Cureus*. 2024;16.
- [16] Mecacci G, Haselager P. Five criteria for assessing the implications of nta technology. *AJOB neuroscience*. 2019;10(1).
- [17] Levy S. Hackers: Heroes of the computer revolution. Doubleday: New York (1984).
- [18] Bellaby R. An ethical framework for hacking operations. *Ethical Theory and Moral Practice*. 2021;24.
- [19] Coleman E, Golub A. Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory - ANTHROPOL THEORY*. 2008;8.
- [20] Warusfel B. Contre-espionnage et protection du secret : Histoire, droit et organisation de la sécurité nationale en france. Panazol: Lavauzelle (2000).
- [21] Allison B. Why bci-fi? In: *Proceedings of the 10th International Brain-Computer Interface Meeting*. 2023.
- [22] Iacono W, Ben-Shakhar G. Current status of forensic lie detection with the comparison question technique: An update of the 2003 national academy of sciences report on polygraph testing. *Law and Human Behavior*. 2018;43.
- [23] Sifaoui A, Eastin M. “whispers from the wrist”: Wearable health monitoring devices and privacy regulations in the u.s.: The loopholes, the challenges, and the opportunities. *Cryptography*. 2024;8:26.
- [24] Welter M, Lotte F. Ecological decoding of visual aesthetic preference with oscillatory electroencephalogram features—a mini-review. *Frontiers in Neuroergonomics*. 2024;5.
- [25] Gidaris C. Surveillance capitalism, datafication, and unwaged labour: The rise of wearable fitness devices and interactive life insurance. *Surveillance & Society*. 2019.
- [26] International A. The social atrocity: Meta and the right to remedy for the rohingya. London, 2022.
- [27] Ziogas A et al. Deep learning in the identification of electroencephalogram sources associated with sexual orientation. *Neuropsychobiology*. 2023;82.
- [28] Galli G et al. Early eeg responses to pre-electoral survey items reflect political attitudes and predict voting behavior. *Scientific Reports*. 2021;11:18692.
- [29] Dorsey J, Bo M. Ai-enabled decision-support systems in the joint targeting cycle: Legal challenges, risks, and the human(e) dimension. *International Law Studies*. 2026;107(1).
- [30] Robertson L, Higgins NL, Maier MJ, Carter A, Gardner J. Ethical governance strategies for the responsible innovation of neurotechnologies: A scoping review. *Journal of Bioethical Inquiry*. 2025;22.
- [31] Scarfone K, Jansen W, Tracy M. Guide to general server security. recommendations of the national institute of standards and technology. 2008. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/123/final>.
- [32] Wachter S. Limitations and loopholes in the eu ai act and ai liability directives: What this means for the european union, the united states, and beyond. *SSRN Electronic Journal*. 2024.
- [33] Observatory CE, LobbyControl. Article by article, how big tech shaped the eu’s roll-back of digital rights. 2026. [Online]. Available: <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>.
- [34] Krempel S. Setback for the commission: Eu meps let chat control fail. *Heise Online*. 2026.