Review Article

DIGITAL HEALTH

DIGITAL HEALTH
Volume 11: 1–19
© The Author(s) 2025
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20552076251326123
journals.sagepub.com/home/dhj
Sage

Regulating neural data processing in the age of BCIs: Ethical concerns and legal approaches

Hong Yang and Li Jiang

Abstract

Brain-computer interfaces (BCIs) have seen increasingly fast growth under the help from AI, algorithms, and cloud computing. While providing great benefits for both medical and educational purposes, BCIs involve processing of neural data which are uniquely sensitive due to their most intimate nature, posing unique risks and ethical concerns especially related to privacy and safe control of our neural data. In furtherance of human right protection such as mental privacy, data laws provide more detailed and enforceable rules for processing neural data which may balance the tension between privacy protection and need of the public for wellness promotion and scientific progress through data sharing. This article notes that most of the current data laws like GDPR have not covered neural data clearly, incapable of providing full protection in response to its specialty. The new legislative reforms in the U.S. states of Colorado and California made pioneering advances to incorporate neural data into data privacy laws. Yet regulatory gaps remain as such reforms have not provided special additional rules for neural data processing. Potential problems such as static consent, vague research exceptions, and loopholes in regulating non-personal neural data need to be further addressed. We recommend relevant improved measures taken through amending data laws or making special data acts.

Keywords

Neural data, brain-computer interfaces, privacy, data processing, regulation

Submission date: 14 June 2024; Acceptance date: 20 February 2025

Introduction

Brain–computer interface (BCI) technologies have developed at an increasingly rapid speed. The first human brain-chip implant was conducted in the beginning of 2024 by Neuralink.[1] BCIs may help patients who are paralyzed or non-verbal to regain free movements and words communication, and have also rapidly expanded to the consumer sphere with educational and recreational applications.[2]

BCIs collect and process data from our brain activities, termed as "neural data" or "brain data" interchangeably by a UNESCO report.[3] A broad definition for such data may be found in the OECD Recommendation on Neurotechnology (OECD Recommendations), which defined "personal brain data" as those relating to the functioning or structure of the human brain of an identified or identifiable individual that include unique information about their physiology, health, or mental states.[4] Particularly, "neural data" has been defined in a law for the first time in the newly amended data privacy act of the state of Colorado in the U.S., followed by California shortly afterwards. As the first two regulatory definitions for neural data, both the two acts interpret it with the key element of information generated by measuring activity of "central or peripheral nervous systems."[a] Besides, a broader concept of "cognitive biometric data" is used by some experts referring to neural data as well as other data collected from a given individual or group of individuals through other biometric and biosensor data.[5] Despite the different terms used and angles of definition in different discussive backgrounds, we take an inclusive approach and use in this article the term "neural data" as covering those information generated from human nervous system or other cognitive

Shanghai International College of Intellectual Property, Tongji University, Shanghai, People's Republic of China

Corresponding author:
Li Jiang, Shanghai International College of Intellectual Property, Tongji University, 200092 Shanghai, People's Republic of China.
Email: jiangli36@tongji.edu.cn

system, so as to embrace different studies and legislations. But we emphasize that neural data of concerns may also involve non-personal data generated through inferences or analysis.

While providing great benefits for wellness and scientific progress, BCIs also raise significant concerns regarding challenges for privacy, integrity, and safety of our neural data. Studies have shown that such data may be used to infer visual content of mental processing, covert speech, or even reportedly to predict future tendency of carrying out certain acts (e.g., criminal tendency).[6] Warnings have been discussed about unauthorized access,[7] sensitive inferences and predictions about individual and group information,[8] motivation for purchasing,[9] and unwanted surveillance and manipulation.[5] Combined with other advancing technologies, the rapid development of artificial intelligence to decode and analyze neural data brings us closer to mind-reading in reality.[10]

Such challenges and risks are not pure theoretical speculations, echoed by relevant attempts in business activities. It has been reported that Kernel, a multimillion-dollar company wants to "hack the human brain," which is joined by Facebook wanting to develop a means of controlling devices directly with data derived from the brain.[b] The new launch of Neuralink has created more potential and uncertainties for the power of new-generation BCIs.[1]

In addition to fast-developing ethical considerations and proposals concerning right to mental privacy under human right context,[11] regulatory response is equally important and possibly more immediate in addressing those new challenges. As a most relevant field to neural data, data protection laws such as the GDPR[12] provide specific rules for regulating data processing, which might provide a mature legal basis for oversight of neural data exploitations. Under the category of sensitive data in GDPR, health data cover personal data related to physical or mental health, and biometric data relate to physical, physiological or behavioral characteristics of a person, which allow or confirm the unique identification of that person. Both two types of existing sensitive data may partially cover neural data. However, there have been various BCIs for recreational or educational purposes such as NeuroSky.[2] They may generate neural data beyond the meaning of health data. Moreover, biometric data is only regulated as sensitive data conditioned upon "uniquely identifying" purposes, while BCI-generated neural data may constitute personal data yet without bearing those direct purposes. Accordingly, current regulatory approaches for classifying sensitive data represented by GDPR are not fully responsive to new data issues of BCIs. Neural data are "uniquely sensitive,"[5,6] posing unique risks which might not have been envisioned by conventional legal approaches in data laws. With most current data laws worldwide not yet mentioning neural data, it has been observed that existing information protection regimes are potentially insufficient for adequately safeguarding mental privacy,[13] and that "beyond GDPR" there are further BCI-related data concerns.[14]

In this article, we elaborate on the specific legal approaches concerning neural data protection in furtherance of existing proposed solutions focusing on ethical and human right dimensions. We propose that data laws might be the most suitable and enforceable legal system to efficiently regulate neural data processing, with needs to reform certain aspects taking full account of specialty of neural data and BCIs. We begin with analyzing new functions of BCIs and their impact on neural data. Then, we explore the specialty of neural data and summarize main ethical concerns widely discussed, finding the core role of data laws to realize and implement proposed ethical guidelines. Under that premise, we review current regulatory systems and legislative reforms, especially including those of the two U.S. states of Colorado and California specifically covering neural data. We then analyze existing legal approaches, especially potential problems not yet solved considering the special features of neural data and BCI applications. Finally, we raise recommendations in response to relevant regulatory gaps we identified.

Impact of BCI technologies on neural data

BCIs can be invasive (chip implanted in brain) or non-invasive (wearable device such as a helmet).[2] They have the functions of both "reading-out" through an "electroencephalogram" (EEG) and "functional magnetic resonance imaging" (fMRI) and "writing-in" through electrical or optical stimulation; reading out BCIs may decode brain signals using algorithms and formulate specific inferences about the user's brain activities or thoughts, individually or in combination.[15]

Both invasive and non-invasive BCIs may access and decode mental processing,[2] thus capable of analyzing neural data. Due to the intense activity 24/7 of the brain, neurotechnology may collect many types of neurodata.[16] With a neuroscientist noting that AI and machine-learning algorithms "turbocharged the whole field," BCIs may at least partially realize the ever-long fantasy about "mind reading" and even "changing minds."[17] Examples include a study that demonstrated speech decoding from neural data from the sensorimotor cortex using deep-learning models and EEG technology and decoded words in reconstructed speech with 92%–100% accuracy, as well as a study where researchers decode a Pink Floyd song which participants were listening to by analyzing their neural activity with generative AI.[2] Moreover, a study using fMRI scans of deep neural networks to reconstruct mental images from brain activity achieved accuracies of 90% for seen images and 75% for imagined images.[2]

On the one hand, BCIs development create great benefits for treatment of neurological illnesses, as well as new application scenarios for educational and recreational purposes. On the other hand, it brings about unprecedented and uncertain challenges and risks for the integrity and privacy of neural data. Neural data may be used to infer not only individuals' physical health but also the mental state, including problem-solving, reasoning, decision-making, memory retrieval, perception, and emotions.[16] Using decoding techniques especially algorithms, BCIs may further "read" the brain data generated, deducing alterations in intentions, behaviors, and cognitive states.[15] Experimental results suggested that the extraction of specific PIN codes from EEG signals is theoretically feasible for some users and PINs.[18]

Particularly with the ever-advancing BCI technologies, novel spywares and cyberattacks are more likely to be explored against neural data. It is possible to design malicious applications with which EEG signals collected for gaming can be used to reveal other types of correlations, such as medical or political ones.[13] Security vulnerabilities have been identified through the new micron-scale BCI, where scientists experimentally simulated two types of neuronal cyberattacks, respectively neuronal flooding (FLO) and neuronal scanning (SCA), and found that both cyberattacks are adequate to affect neuronal activity, with FLO being more effective in immediate terms and SCA in the long term.[19]

Ethical concerns for the uniquely sensitive neural data and legal approaches in response

From ethical perspectives especially including human dignity, self-determination, and privacy, neural data exhibit unique characteristics which do not appear to be mirrored by conventional forms of data. Researchers have argued that neuroscience data are particularly more sensitive than are other personal or health data due to their intimate nature.[6] First, neural data touch on the "locus internus,"[8] or the most private sphere of human mind. Being the "last refuge" of freedom and self-determination, our minds along with thoughts, beliefs, and convictions, are "fortresses" largely beyond external constraint, in contrast with body which is easily subject to domination and control.[20] Neural data are more proximal to personhood compared with other data, and may unveil one's "subconscious tendencies and biases" not filtered through executive control.[7] They closely reflect who we are, thus even considered to have philosophical relevance and moral importance to one's identity.[20]

Second, neural data are multidimensional. They concern both mind integrity and psychological integrity.[21] As introduced above, neural data may even help infer behavioral data predicting future actions tendency. Third, neural data are variable and fragile. It is still unclear regarding the construction of the brain–body–mind relationship.[22] BCI-generated data may manifest our unknowingly or unintentionally revealed thoughts, emotions and even personality. They may provide insight into an individual which might even be unknown to or out of control of the individual.[23] BCIs may even generate ability to control one's thoughts and lead to manipulation of one's sense of agency or personal identity.[7,24]

Even compared with other types of sensitive data such as genetic data or biometric data, neural data involve particularity. Genetic data, fingerprint, and other biometric data tell about external individuals such as what we look like, while neural data tell about internal individuals such as what we are thinking.[25] Just as a scholar argues, "I already don't want my employer or insurance company to know my genome. As to my brainome, I don't want anyone to know it for any purpose whatsoever. It is … my most intimate identity."[26]

Ethical considerations related to the uniquely sensitive neural data have long developed, with the growing concerns for BCIs among brain technologies.[27] They originated from concerns of neurotechnology generally, covering a wide spectrum of aspects identified by a thematic analysis as amounting to 24 issues ranging from accountability to trust.[28] Back in 1993, the UNESCO had founded an International Bioethics Committee (IBC), which started exploring ethics in neuroscience.[29] The International Neuroethics Society (INS), formed by multidisciplinary experts indicates that neuroethics involves ethical concerns well beyond bioethics.[c] The IBC issued a special report for ethical issues of neurotechnology in 2021, recognizing most important ethical principles such as mental integrity and human dignity, personal identity and psychological continuity, autonomy, and mental privacy.[3] An Ad Hoc Expert Group (AHEG) was further constituted by the UNESCO Director-General to draft a "Recommendation on the ethics of Neurotechnology," and a first draft version (UNESCO Recommendation Draft) was issued in 2024.[30]

Among broad neuroethical concerns for both physical and mental aspects, mental privacy may be said as the special priority in respect of BCI-generated data, as privacy is the foundation for data protection. Ethical concerns about privacy and unauthorized access of neurotechnologies are pressing, especially with their putative capacity.[31] The IBC ethics report dedicated a special section on BCIs and raised data risks under the notion of "mental privacy," summarizing "mind reading" as a risk for mental privacy, where data may be unexpectedly detected, and access to neural data by third parties may have consequences.[3] As consumer neurotechnology gains steam, ensuring that privacy standards are acceptable remains a challenge.[17]

The ethical research and guidelines for neural data, or neuroethics related to privacy, play an important role as an ethical basis for regulating neural data processing. Protecting data subjects' interests requires the identification of sufficient ethical considerations for privacy, including the value of individual data ownership, the extent and degree of uniqueness of neural data as discussed above, balancing interests of neurotechnology companies involving difficulties in anonymization, strengthened cybersecurity measures, etc.

Nonetheless, neural data under BCI technologies take the form of generated and analyzed data, where data protection, or vis-à-vis, regulating of its processing, is a regulatory system beyond mental privacy as a fundamental human right. The INS mentioned brain data protection as one of the main aspects where neuroethics differ from bioethics.[b] Multiple studies covering mental privacy have also actually focused on legal rules related to neural data processing.[15,24,28] Moreover, ethical guidelines set up values and principles, while further implementation with a binding force is still needed through regulatory systems for data processing. As noted by social scientists, ethics "shape laws" while laws "complement" it.[32] Some scholars have been skeptical that ethical self-regulation of neurotech firms will seriously ever put the brakes on mind-reading devices, when there is so much lucrative personal data to harvest.[33] We believe that ethical principles are important for the governance foundation of neural data, while they need to be further addressed by specific legal approaches in the form of regulatory systems for data processing. Further to those ethical concerns expressed about relevant mental privacy risks, the regulation of neural data processing through corresponding legal approaches addressing those concerns in response is distinct and indispensable. Therefore, we will mainly review regulatory approaches involving neural data in the form of data laws. Considering the analysis about particularity of neural data, we hold that in evaluating such regulatory approaches for addressing relevant new ethical concerns, neural data should be treated as "uniquely" or "highly sensitive" as identified by the IBC report,[3] even compared with conventional types of sensitive data such as biometric data.

The status quo: Existing regulatory approaches and recent legislative reforms

Neural data are "inherently identifiable,"[6] thus being highly likely to constitute personal data. Under GDPR and the recent case standards of the Court of Justice of the European Union (CJEU) in *Nowak*[34] and *Breyer,*[35] personal data cover any information with the capability of a "link" with the person. Such an "expansive" approach means that even passive BCIs like EMOTIV's MN8 only monitoring certain brain activities might be seen in analogy with the case of *Nowak* and involve personal data processing.[14]

Typical personal data laws and relevant reforms for neural data

Following the comprehensive data protection/regulation rules of GDPR treated as the "gold standard,"[36] typical personal data protection laws have been developed in major economies, including the Personal Information Protection Law (PIPL) in China.[37] The United States has not yet established a federal personal data law yet has provided a legal system of HIPAA for health data as early as 1996.[38] Moreover, typical state data privacy statutes were launched with standards corresponding to GDPR, such as the California Consumer Privacy Act (CCPA) as amended in 2020 (CPRA).[39] However, none of the typical data laws passed before 2024 had clear coverage of neural data per se. Meanwhile, most data laws have a special category of sensitive data under stricter protective rules, especially involving health data and biometric data which may partially cover neural data.

As an important breakthrough, the U.S. state of Colorado amended the Colorado Privacy Act (CPA) in 2024[40] and became the first comprehensive data law worldwide to explicitly protect neural data.[d] Shortly afterwards, California also made a new amendment to CCPA, similarly bringing neural data under its regulatory scope.[41]

As demonstrated in Table 1, both the two newly amended data laws clearly listed neural data under the category of sensitive data as a subject matter with specific definitions. The CPA places neural data under "biological data," being subject to a limited scope of only those "for identification purposes." In comparison, the new CCPA does not have such a precondition. Notably, both of the recent amendments for CPA and CCPA took place shortly after their last revisions, which may reflect their recognition of the urgent need for protecting neural data independently.

With more sophisticated regulatory approaches, Minnesota introduced a new bill (Minnesota Neurodata Bill) providing additional protection for neural data.[42] China has not clearly added neural data in the PIPL, but recently issued an ethical guideline specially for BCI research, encompassing data use. Although being departmental rules, it has certain binding effect linked with regulations about biological and medical research related to human beings.[43] The U.S. Food and Drug Administration (FDA) also issued a guidance for implanted BCI devices. But it is limited to devices under the scope of medical purposes and does not focus on data processing. Importantly, it only comprises "nonbinding recommendations."[44] In Table 2, we summarize the typical approaches in reformed data laws and regulatory systems, including the newly passed AI Act of EU.[45] Although the newly reformed CPA and CCPA clearly added neural data under protection, they have not provided any specific rules accommodating the special features of such data. On the contrary, some other new regulatory systems impose additional regulatory rules related to neural data.

The Minnesota Neurodata Bill is probably the first legislative attempt of its kind to provide specific rules protecting neural data in addition to incorporating it into sensitive data. China's ethical frameworks specially for neural data is also special in this regard, especially with similar emphasis on consent and pre-examined scope of use purposes, yet with a limited scope only applicable to research activities. EU's AI Act indirectly covers neural data through regulating "emotion recognition system," but it is based on biometric data defined with condition on "identification" of natural persons.

Specifically, processing involving third-party sharing and further repurposing are extremely influential on neural data.

Table 1. Typical personal data laws and legislative reforms involving neural data.

Personal data laws	Neural data listed under sensitive data	Neural data listed under a broader category	Health and biometric data covered under sensitive data	Biometric data conditioned upon identifying purpose
Typical data laws before 2024				
EU: GDPR adopted in 2016	No	No	Yes	Yes
USA: CCPA as amended by CPRA 2020	No	No	Yes	Yes
China: PIPL adopted in 2021	No	No	Yes	Yes
Reformed data laws since 2024				
USA: CPA as amended in 2024	Yes. With clear definition	Yes. As a subcategory of biological data, with precondition of "identification purposes"	Yes	Yes
USA: CCPA as amended in 2024	Yes. With clear definition	No	Yes	Yes

Existing data laws like those of the EU, the United States, and China have provided certain special rules in that regard, while each embodying different approaches.

As shown in Table 3, the GDPR sets an "opt-in" right of consent for processing of any data including sensitive data, with "processing" embracing third-party sharing. It does not require a new consent regarding even sensitive data sharing, yet providing informing obligations and corresponding right to opt out through withdrawal of consent or erasure. Sharply in comparison, China's PIPL asks for a separate consent for any third-party sharing, as well as for any type of processing of sensitive data. The CCPA is somehow in between the previous two approaches. As most American privacy laws do not require consent as a general lawful basis, there is a presumption that personal data may be used or disclosed unless a specific rule forbids it.[46] But the CCPA provides strengthened opt-out right to limit use or disclosure of sensitive data only to rather limited scenarios like necessary technical support or maintenance. As for repurposing of data processing, the GDPR only prohibits "incompatibility" for further processing while China's PIPL asks for a new consent for any "changed" purpose. Both the GDPR and CCPA set up research as exception, while the PIPL has no research exception for any data processing. While GDPR imposes it specially on sensitive data processing without specific definition, the CCPA uses a restrictive approach to confine types of research exceptions as well as providing a specific definition for research.

Non-personal data regulations

Another type of data in addition to personal data should not be neglected, involving non-personal neural data which do not contain personal data or have been anonymized in a way not linkable to any individual. The EU has set up preliminary frameworks for non-personal data. Firstly, the Data Governance Act (DGA) adopted in 2022 regulates the use and sharing of "public-sector" held data of both personal and non-personal nature.[47] Secondly, EU issued a proposed Regulation on European Health Data Space (the EHDS Proposal), which aims at promoting sharing of personal and non-personal health data.[48] The DGA empowers legislative acts to deem certain non-personal data categories to be "highly sensitive," and imposes requirements and conditions for international transfer of such data. The EHDS Proposal further quoted DGA to pose requirements on international transfer of non-personal health data, especially concerning risk of re-identification.

Taking a stronger approach, China passed a Data Security Law in 2021, which covers "important data" referring to certain non-personal data held by not only public bodies but also enterprises, the leak of which would cause potential injuries to national or public interests. A "Catalogue for Important Data" is delegated to list types of important data, and cross-border transfer of such data is subject to security review by competent authorities.[49] Although this general catalogue has not been issued due

Table 2. Reformed data laws and new regulatory guidelines protecting neural data.

Regulatory approaches for neural data	Affirmative protection and definition	Special rules regulating neural data processing
USA: CPA (2024)	Yes. Based on measurement of activity of central or peripheral nervous system linked with a device	No
USA: CCPA (2024)	Yes. Based on measuring activity of a central or peripheral nervous system, not inferred from nonneural information	No
USA: Minnesota Neurodata Bill (2023)	Affirmative protection: Yes. Specific definition: No (With definition for BCIs).	1. An independent notice required for each time of BCI connection, covering information about: (1) type of uses; (2) third parties to be shared with. 2. A separate consent for each use and third party shared with, using a separate consent form. – Sec.2, Subd. 3.
EU: AI Act (2024)	No	1. Emotion recognition system: AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. 2. Prohibited AI practices: AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except for medical or safety reasons. 3. High-risk AI system: emotion recognition AI other than those prohibited is subject to risk management and monitoring measures. – Art. 5.1 (f), 6 (2).
China: Ethical Guideline for BCI Research (2023)	Affirmative protection: Yes. Specific definition: No (With definition for BCIs).	1. Mandatory ethical review: limited to BCI research with clinical research purposes. 2. Special Ethical review procedure: Scope of neural data collected and authorized access subject to review by an Ethics Committee. – Art.4.4 3. New consent for participation required where new circumstances are discovered involving risky information or possibly influencing the participant's will. – Art.4.3

to extreme complexity of identifying types of important data, there have been sectoral regulations in the field of automobile data, indicating such data as covering military geographical locations, operation of electricity charging network as important data.[50] As a countervailing balance, the implementing regulation newly issued in 2024 for the Data Security Law prevents a vague interpretation for important data and makes clear that enterprises are not obligated to do self-assessment about whether they are holding such data, thus not bound to apply for a security review unless the data held is within the catalogue or is informed by competent authorities to be of concerns.[51]

Special implications of reformed data laws as compared with the newly proposed "neuroright"

Among the increasing number of regulatory reforms involving neural data which emerged recently, those in the United States have highly important and special implications. Firstly, they are all designed within more enforceable data law frameworks specializing on data regulation in comparison with sectoral rules that usually lack comprehensive measures for data issues. For example, the new prohibited acts for emotion recognition system in the EU AI Act are limited to scenarios of workplace and education institutions. Secondly, two of them have shaped into effective laws in furtherance to ethical guidelines or neurorights which substantially stay at the stage of proposals. An industry report also indicates that policy makers should draft not only standards and best practices but also pragmatic regulations which are neurotechnology specific.[52] It is especially necessary to note the special meaning of data law framework and its reforms in comparison with another legal approach in parallel, namely the newly proposed neuroright embracing the proposed right to mental privacy which also closely relates to neural data.[20]

Table 3. Consent and exceptions in respect of sharing and repurposing.

Data laws	Consent as lawful basis for third-party sharing	Consent for repurposing	Research and other flexible exceptions to consent	Special protection for sensitive data
GDPR (2016)	Yes. 1. Opt-in model at initial collection. – Art.6 2. No requirement for additional or separate consent specially for third-party sharing. 3. Requirement for informing obligations for third-party sharing, coupled with opt-out right to withdraw consent and right to erasure. –Art.7.3, 14, 17.	New consent not required unless with further processing "incompatible" with initial collecting purposes (purpose limitation). – Art.5.1 (b)	1. Two set of exceptions (to consent/prohibition): (1) Non-sensitive data: "contractual necessity," "legitimate interests," etc., not including research. (2) Sensitive data: research is exception to general prohibition or explicit consent, subject to flexible safeguards like pseudonymization. Contractual necessity and legitimate interests are not included. –Art.6 (b) (f), 9.2, 89.2 2. Research purpose is exception to "purpose limitation," not constituting "incompatibility" – Art.5.1 (b). 3. No definition for research.	1. Opt-in right with additional requirement for consent to be "explicit." – Art. 9.1 2. More specially limited set of exceptions.
CCPA (2024)	No. 1. Limited opt-out model: consumer's right to prohibit sale/ sharing upon processor's obligation to notice and to provide "Do Not Sell or Share" weblink. – Sec.1798.120 2. Processing other than sale/ sharing is still permitted, unless for sensitive data, or through general right to delete. – Sec. 1798.105	Prohibiting additional purposes "incompatible" with initial collection purposes. – Sec.1798.100	1. Medical or health information under regulations like HIPAA; 2. Clinical trial and biomedical research conforming to good practices, otherwise requiring a separate consent. – Sec.1798.145 3. Clear definition for research: limited to those contributing to public or scientific knowledge, with public interests or operational purposes under additional security control. – Sec.1798.140	Strengthened opt-out right: right to limit disclosure to those necessary for providing services or goods, reasonably expected by an average consumer, in order to perform limited tasks of security, transient use or maintenance– Sec.1798.121, 135
PIPL (2021)	Yes. Additional opt-in right for third-party sharing, with a separate consent required. – Art. 23	Renewed consent required for any "changed" purposes. – Art.14.2	No. 1. One set of exceptions for any data, including contractual necessity. 2. Research is not exception either generally or specially for sensitive data. – Art. 13.2	Separate consent required for any processing of sensitive data. –Art.29

As a practice reflecting the spirit of neuroright (but not exactly identical), Chile became the first country to add protection related to neural system by amending its constitution in 2021, which requires that technological development respect mental integrity and that the law must protect brain activity and information related to it.[53] In the case *Girardi v. Emotiv Inc*, the Chilean Supreme Court referred to that constitutional amendment and held that the State is expected to act "in order to prevent possible effects of new technologies, directly protecting human integrity including privacy and confidentiality." It thus ordered that the defendant company delete the plaintiff's brain information from its database, and that the product be assessed by relevant authorities before its commercialization. Nonetheless, the plaintiff's claim for the defendant to modify its privacy policies before selling the product was not wholly supported.[54] The "Emotiv case" still leaves many important issues unresolved. It only provides protection in principle for fundamental right of mental integrity, not treating specifically issues of data processing. Since neural data is a form of data in addition to fundamental rights, that neuroright-type protection is not yet ready for specific implementing rules, especially those relating to requirements about scope and types of protected neural data, consent for data collection/sharing, and justified exceptions. Consequently, such an approach cannot provide specific data obligations for neurotechnology businesses, particularly unable to regulate their privacy policies which are crucial for protecting neural data. The failure of the Chilean supreme court to rule about the privacy policy issue also reflects the limitation of such protection through human rights or similar fundamental rights.

In contrast, reformed data laws like the CPA and CCPA provide a more suitable legal approach to achieve those regulatory tasks which are left blank by the "Emotiv case." BCI-generated data involve protection of data rights on the one hand and legitimate data use for public interests on the other hand. Relevant policies should balance the promotion of technological innovation with the imperative to protect mental privacy.[30] This demands sophisticatedly enforceable rules regulating specific aspects of neural data processing as an extension to fundamental human rights, including those measures for control for data sharing and justified exceptions ensuring the abovementioned balance. As observed, the new human right needs to be introduced through international negotiations, and consensus is not easy to achieve.[55] The legislative reform regarding current rights could be a better solution.[56] Brain data protection under the new risks may fit within existing legal privacy frameworks such as GDPR, where we can better conceptualize the new risks by applying the latest theories in information privacy.[57]

Taking account of that important background, the new reforms of CPA and CCPA create an important breakthrough. Being the first two data laws worldwide specifically incorporating neural data as an independent subcategory under data regulatory frameworks, they employ the data privacy rules to protect neural data specifically. Although neural data may have been considered by some in past practices as falling under certain type of existing data, the newly reformed data laws like CPA and CCPA move forward by clearly categorizing it as sensitive data. Notwithstanding the variations between CPA and CCPA regarding sensitive data, they both set stricter requirements for processing such data. A higher standard of "opt-in"[40] or strengthened "opt-out" right[39] is required for sensitive data compared with those general "opt-out" right for general data. Besides, the CCPA imposes a more rigid limit on use/disclosure and opt-out preference choices for sensitive data,[39] while the CPA requires the controller to specially conduct a data protection assessment for sensitive data.[40]

Such regulatory reforms may produce deep influences for neurotechnology companies, as neurotechnology companies in Colorado and California will need to switch their business model and especially their privacy policies which did not treat neural data specially to those recognizing the sensitive status of neural data. According to a report surveying privacy policy of 30 companies prior to the reformed data laws, there is enormous ambiguity regarding whether companies consider neural data even as a form of personal data. Furthermore, their data collection and storage practices are ambiguous, and almost all of the companies can share data with third parties, with the extent to which they can sell data being unclear.[2] With the two reformed data laws taking effect, BCI businesses operating in the two states will have to change their data processing practices to treat neural data specifically as sensitive data, as well as to meet those corresponding special requirements. This will particularly involve modifying their privacy policies so as to specifically provide special procedures of data collection and sharing for neural data, an area not addressed by the "Emotive case" in Chile. Those problems regarding neural data in current privacy policy and data practices of BCI companies will at least partially be ameliorated.

However, from a view of precaution, the effects of the reformed CPA and CCPA may still be limited. Neural data has unique features and associated risks even compared with other types of sensitive data as discussed earlier. Custom-made regulations not relying on shoehorning brain data into preexisting terms within privacy protection regimes are needed, and new legislation like the CPA highlights the "emerging necessity" for more explicit guidance in privacy laws regarding neural data.[13] The CPA and CCPA reforms only stop at bringing neural data under the category sensitive data. Beyond those broadly applicable requirements for all types of sensitive data as a whole, there are no further special rules considering those unique features and risks related to neural data. Thus, the current data law reform approaches may need further development to add strengthened requirements such as those about consent, dynamic disclosure, and security measures, which are responsive to the specialty of neural data as well as new challenges associated with BCIs. In this regard, the Minnesota Neurodata Bill might represent a more revolutionary and precautionary effort than the approaches taken by CPA and CCPA. It is "unique" in that it requires additional measures such as an independent notice and a separate consent for "each use" and each "third party shared with."[42]

Issues with current regulatory approaches: Potential problems considering challenges from BCI applications

Except for the two newly amended data laws of CPA and CCPA, the GDPR and most existing data laws have not covered neural data as an independent type. Even the new CPA and CCPA have not gone further by adding any new special rules considering the special features of neural data. The fast-growing BCI technologies may incur new types of data risks and thus require further regulatory approaches in response from a data regulation perspective. A study expressly asked whether the level of strong protection of medical data is sufficient, demanding that intimate brain data should enjoy stronger protection.[14] Consistently, some scholars have urged creating legislation specifically designed to protect neural information privacy.[13] Accordingly, potential problems of existing legal approaches need to be further explored specifically.

Incomplete coverage for non-medical or non-identifying BCI-generated data

Due to the lack of neural data listed independently in most existing data laws, the complete coverage for neural data is limited despite possible existing types that may partially encompass it. Although health data as a type of sensitive data might partially cover neural data, some are generated in a non-medical context. If brain data stems from consumer neurotech and recordings of the type envisioned by Facebook, Kernel, and Neuralink, the data might seem not to constitute "health data."[14] Existing data laws including the HIPAA may not fully apply to data collected outside traditional medical or healthcare contexts.[5] Importantly, there have been strict or heightened requirements for medical devices and health privacy.[2] However, the recreational and educational BCIs may evade such heightened requirements while they face risks equal to medical BCIs in respect of generating neural data.

As for biometric data as another type of existing sensitive data, current data laws including the new CCPA were framed upon ability to identify an individual based on biometric data, leaving "biometric psychography" and accompanying inferences produced through BCIs potentially not to be interpreted as covered under these laws.[52] More generally, the CPA's coverage of neural data itself is subject to a limitation of "identification purposes," commented as "significantly limiting the protections."[5] Even though the new AI Act touches novel regulatory considerations for "emotion recognition," it is still limited to the "identification" premise of biometric data, and the main measures are limited to specified non-medical scenarios of workplace and education.[45] More lenient measures for other high-risk emotion-related AI appear not to extend to the "decoding of non-affective" mental states such as cognitive and conative states.[5]

Static consent for repurposing and third-party sharing

Although the GDPR has an additional requirement of "explicit" consent specially for sensitive data, it still concerns more about the formality of expressing a consent. The risks for neural data generated by BCIs firstly concern more of the uncertain future uses or the repurposing of processing such data. Health applications may process data for training AI algorithms,[58] where app users may not realize that they have given an ambiguous consent to such repurposing.[59] As noted, just a "subset" among the large amount of brain data generated by BCIs is directly relevant for operating the devices, with a remainder of "data exhaust," and the data superfluous to the specific purpose could simply "bypass" the GDPR.[14]

Existing data laws usually do not clearly exclude flexible and broadly inclusive statements about purposes for processing. Although the GDPR has requirements about "freely given" consent based on specified purposes,[12] the consent is still given in a static and "once for all" manner. As the bill newly amending CPA expressly states in its legislative declaration, neural data collection always involves "involuntary disclosure," and even if individuals consent to processing for a narrow use, they are unlikely to be fully aware of the content or quantity of the information, or to understand the extent to which their neural data can be decoded in the future; the information collected may even cover those the individual did not know existed.[40] It has also been asked earlier, "how a static agreement could account for an open future of possibilities is very unclear."[14] This issue is particularly prominent in the context of medical purposes where neurologically hampered individuals face more troubles in understanding the informed purposes on a one-time basis, not to mention the complexly repurposed processing regarding potentially broadened purposes during the complicated BCIs operations. The OECD Recommendation on neurotechnologies also asks for "clear information" about the potential use of personal brain data, as well as consideration of "special cases of limited decision-making capacity."[4]

The "purpose limitation" under some data laws like GDPR and CCPA might intensify such challenges, with their broad limitation on further purposes only preventing "incompatibility" and thus likely to tolerate a broad scope of repurposing if only not being viewed as incompatible by data controllers. For example, collecting data to optimize the functioning of the device may not be treated as being "incompatible" with the initial purposes, and implicit in the software agreement might be the acceptance of measures to optimize the device, which includes subsequent processing of data amounting to a repurposing.[14] In the context of BCIs, purpose limitation requirement may be "exceptionally difficult" to implement, and much information beyond the "intended purpose" might be processed "collaterally" with the targeted information under original purpose, without data subjects' knowledge.[60] Such an approach leaves possibilities for vague interpretation or even abuses by data controllers engaging in repurposing without a new consent.

The repurposing problems become more complex when concerning further third-party sharing based on a broad initial consent. Earlier surveys in the United States suggest that the disclosure and trading of personal information are the main topic of internet users' concern.[61] Problems are also clearly identified about current practices in pre-checked boxes and assumed consent signed up for use by third parties.[62] Especially with the assistance of AI, neural data may result in information disclosures to unintended parties.[63] In the survey for privacy policy of 30 neurotechnology companies, a controversial case was reported where a primary school allegedly used brain-tracking headsets of a company to monitor the concentration levels of students. The data were transferred to the company's server and relevant teachers, yet without providing to the parents. Despite the company's denial about the allegation, the relevant program was suspended after a report in the media about it.[2] Although it is still unconfirmed whether the device actually had the function of brain monitoring, the concerns about the third-party sharing are worth noting. It is problematic if such sharing exceeds the presumed scope of an initial consent usually obtained through a pre-set agreement. Even under data laws like the CCPA which provides data subjects with a claim not to sell personal data, it does not preclude companies from using that data to target users with advertisements.[5] Considering the above-mentioned risks in repurposing as well as vague room in purpose limitation, data subjects further lack efficient means to continuously monitor the unintended data sharing.

Nonetheless, even the newly amended CPA and CCPA which pioneeringly incorporated neural data into the category of sensitive data have not provided any further measures considering those risks uniquely associated with repurposing and sharing of neural data. The lack of special considerations in current legal approaches and relatively passive status of BCI users, combined with the fast-developing feature of neurotechnologies, pose potentially increasing risks for neural data subjects and further obstruct individuals' ability to notice and remedy possible neglections through such rights as the "right to erasure" and "right to withdraw" which has no retroactive effect.[12]

The strict approach of the PIPL might be of relevance to addressing such problems, whereas it requires a separate consent for processing any type of sensitive data as well as for each third-party sharing. But it applies a new consent for all types of sensitive data in an over-restrictive way, and has not taken any special considerations for neural data processing. The Minnesota Neurodata Bill further echoed such considerations, with stronger requirement of a separate consent for each use and third party.[42] However, it is still unclear whether the "each use" refers to one type of uses of the same nature or exactly the actual use at each time. Besides, the bill has not seen any further progress, subject to uncertain changes.

Broad and vague research exception

The GDPR and similar data laws sets various exceptions to the general prohibition on processing sensitive data. Among them, scientific research is of particular relevance for neural data as neurotechnologies especially BCIs are highly reliant on research. Under GDPR, research constitutes exceptions in various stages. First, it is excepted from the general prohibition on processing sensitive data when certain safeguard measures proportionate to the aim of research are provided.[12] Second, scientific research is an exemption to the "purpose limitation" requirement, meaning that further processing for research purposes will not be treated as incompatible notwithstanding their possible departure from initially stated purposes.[12] Although there is a requirement for safeguard measures to ensure "data minimalization," the exact scope of such measures is vaguely listed in a inexhaustive way.[12] Third, research is also legitimate ground for derogations from key data rights such as right of access, right to object, and right to be provided with information.[12]

With such a strong effect of exemption from data controllers' key obligations like consent and purpose limitation, research has not been delineated under GDPR. The ambiguity of research under GDPR has been observed by both data enforcement bodies and academia. Even the Recital 33 of GDPR admits in itself that "it is often not possible to fully identify" research purposes upon data collection.[12] EDPB further interprets this Recital as allowing a purpose described "at a more general level."[64] Multiple studies recognize research as "legal uncertainties,"[65] and "without clearly explaining them."[66] Regarding the purpose limitation exempted by research in the context of clinical trial under the Clinical Trials Regulation (CTR),[67] EDPB pointed out that there is a "presumption of compatibility" of further purposes for research, which has "horizontal" and "complex" nature requiring attention and guidance in the future.[68] As for the right to information in case of data collection not directly from the participant, it is noted that research exception in this regard will cause a participant not to be aware of such processing, and accordingly not to be able to exercise the right to object, causing limited ability to exercise their autonomous choice with regard to potential use of their data.[69]

Research activities have always been associated with the risks of unexpected data misuse. Earlier in history, there has been case like the Tuskegee Syphilis study, where the collection of individuals' data from the autopsies once they succumbed, actually prevailed the real goal to cure patients.[70] The broad scope of research under the GDPR approach may stimulate the impulse of some research-related activities to explore the room of ambiguity in neural data processing. This is especially noteworthy in scenarios of BCI industry which is highly technology propelled and extremely pioneering, whereas scientific research is more influential as well as being more promoted by and more entangled with commercial or commercially related activities. There is likelihood that brain data processing occurs under "auspices" of "research" by private entities and such data will be used by consumer companies "appealing to" research exemption.[60] At least partially relevant, use for "scientific research" under the EU Directive on Biotechnology Invention has been interpreted by the Court of Justice as covering "industrial or commercial purposes."[71]

In business practice, the survey report for neurotechnology companies shows that the majority of the surveyed BCI companies share data with third parties especially including research affiliates. For example, privacy policy of Myndlift notes that it may share EEG data, cognitive tests results and data of age and health details with other entities for their academic research purposes, after removing directly identifying data such as name and contact. Muse offers voluntary research programs where participates will consent to the sharing of "Muse Data (including EEG data) on a de-identified basis with third parties for research related to improving products." Emotive and some other products also have similar voluntary programs involving data sharing with researchers.[2] Even if such policies provide for preconditions about deidentification or removing directly identifying data, such techniques (especially the latter) are still vague and cannot guarantee strict standard of anonymization or prevention of reidentification. Besides, such conditions usually only apply to data sharing, leaving other data processing like repurposing and storage uncovered. Most importantly, such common practices in relevant privacy policies all take the form of standard format clauses and provide no definition for exact scope of research purposes. They show the widespread motivations of BCI companies to process data for broad research purposes under vague terms. Although possibly based on consent according to GDPR or on opt-out rights according to CCPA, they leave ambiguity on the specific scope of the informed purposes, and further much room for data controllers to exceed the originally scope and types of informed purposes. Considering those scenarios other than data sharing which are not covered by consents, as well as the strong motivation of processing under broad research grounds, a wide uncertain space is left for unexpected or unconsented uses of neural data, which might yet be justified by equally broad research exceptions under GDPR and similar data laws.

From the perspective of researchers, it may be argued that they have a natural and justified motivation for data sharing including those with a commercial connotation, where researchers might also have commercial interest needing to be balanced against privacy.[72] There have been further arguments that individuals in health care system have a "reciprocal duty" for not to oppose credible collection and analysis of their data,[73] or that data-sharing is an "ethical duty" of researchers, in order to "maximise" the contribution of human subjects.[74] A survey for researchers in neurological field shows that, even for such researchers themselves, the majority were at least slightly concerned about potential harm if individual's research data were misused (65%). Particularly, investigators with more easily reidentifiable data and neural data were more concerned about the likelihood of misuse of research data.[75]

Notwithstanding the credit to certain justified interests of researchers, greater transparency for research purposes has been clearly called for in the context of brain data.[76] In any event, a vaguely broad scope of research needs to be avoided in the context of BCI-generated data, application of which has growing uncertainty and unpredictability.

Sharing and cross-border transfer of non-personal neural data

Under certain neurotechnologies, the algorithm for machine learning with neural data would only share certain non-personalized, inferences on the data with a central server for further data processing.[77] BCI-generated data may be treated as not to be personal data after anonymization under GDPR,[12] or as "de-identified" information under U.S. privacy statutes, including HIPAA which specially governs health data.[6] They may also involve inferred or analyzed data such as outcome of assessment,[78] which sometimes do not contain personal data. The earlier ECJ decision also recognized that analysis of an individual is not 'in itself' personal data even though it contains personal data.[79]

Generally, current "privacy laws" carve out de-identified data.[52] Unlike personal data laws which have shaped into comprehensive systems under the model of GDPR "gold standards", non-personal data regulations are only at preliminary formation period, with scattered practices in limited number of jurisdictions. Moreover, newly developed non-personal data regulatory frameworks, including DGA and the EHDS Proposal, have not placed any special concerns on non-personal neural data, leaving anonymized inferred data at large. Processing of non-personal neural data concerns special risks in the context of less regulation at a preliminary stage.

First, anonymized or de-identified data still face the possibility of re-identification, especially when AI and algorithms equip neurotechnologies with more power of decoding and inferring. With the advance in machine learning, brain data though appearing not to identify a data subject may, upon repurposing or in combination with other data, identify a subject and ground predictions about sensitive dimensions of their identity.[14] Such "re-identification" or "sensitive inferences" risks about individuals' mental states also concern de-identified data aggregated and shared for purposes such as marketing or product development.[5] In the consumer product context, the emergence of direct-to-consumer neural devices increases the risks of reidentification and misuse of brain data.[80]

Second, there are unanticipated challenges about uncontrolled sharing of such data, especially regarding interests of certain groups as a whole. For de-identified and aggregate data, companies often do not need to obtain consumer consent before using these types of data for various purposes.[5] The report surveying privacy policies of various neurotechnology companies found that it is common practice to provide that companies may disclose to third parties information that does not identify the users, "without restriction." For example, Flow Neuroscience informs consumers that in addition to personal information, it "might also store anonymised and aggregated data (which does not identify you) based on the information you provide to us." The report concluded that it is not clear whether all or only some data is anonymized, nor is it clear whether the anonymized datasets include neural data, with companies possibly considering neural data not a form of personal data, leading to a "concerning picture" of sharing neural data without limitation.[2]

Studies have consistently pointed to such problems, observing that preventing the misuse of such derived data (including anonymized data) in unanticipated ways poses a challenge for devising appropriate controls against this phenomenon,[81] and proposing that stricter controls should be included over how de-identified or aggregated cognitive biometric data can be shared or repurposed, recognizing the unique risks regarding misuse.[5]

It is also noticed that target of privacy infringement may be a "group" or a "category" involving predispositions including collective features like illnesses and behaviors.[82] Such risks beyond individuals especially concern neural data related to behavior patterns, where processing of such data may cause discrimination and stigmatization at the group level.[83] Accordingly, discrimination can occur through non-personal data not assessed on a wide variety of people, leading to biased and incomplete datasets. Further, behavior-related data is also of great concern regarding profiling and automated decision making. Research has observed that inferred brain data may not constitute regulated biometric data (conditioned on identifying purpose), involving extracted behavior data which might be used to target individuals.[84] Inferences obtained through neurodata about individuals' preferences and psychology might be left out of GDPR, and automated decision-making based on such inferred data will impact users' content choices or addictive effects, further influencing their commercial, social, and even political behaviors.[85]

Moreover, the cross-border transfer of data is a regulatory issue not limited to personal data, as non-personal data may still involve risks to be controlled like the ones identified under DGA. However, relevant regulatory systems are only emerging and differ much globally. The EDHS Proposal reflected special considerations for international transfer of non-personal health data which may partially involve neural data, but it still lacks whole coverage of neural data in non-medical context like education and recreation. Particularly, the Proposal shows a tendency of promoting non-personal data sharing by stating that "secondary use of non-personal electronic data should also be ensured," as well as establishing an "unrestricted access" system for such data.[48] However, its regulation for relevant risks is limited to the issue of re-identification,[48] not covering other potential problems associated with behavior patterns and psychology prediction mentioned above. In this regard, China's Data Security Law establishes a catalogue control system for regulating international transfer of "important data," which might offer further tool for addressing special risks for certain non-personal neural data. But the comprehensive catalogue has not come up, and existing sectoral catalogues have taken no notion of neural data.

Special cybersecurity measures for BCIs

BCI as a pioneering technology produces new cybersecurity risks about uncontrolled access and unexpected attacks. It is noted that when the users' neural information is accessed externally, it is uncertain whether it will be used for other purposes.[86] Such risks are aggravated by advancing technologies like cloud computing. The lack of interoperability between BCI and cloud computing leads to functional issues of network security, and failure to add new threat defense functions may cause many unpredictable security problems.[86] As most current BCI deployments do not consider neural data protection, BCIs toward interconnected devices generate security concerns which will increase in the near future, while the field of security oriented to BCIs is not yet mature, generating opportunities for attackers.[87] This is further complicated by recent novel BCIs based on nanotechnology, such as Neuralink, attack of which can disrupt the spontaneous activity of neural networks.[88] Such nanotechnology miniaturizing the electrodes implanted in the brain, through FLO and SCA attacks discussed previously, further presents vulnerabilities that attackers could exploit to affect neural activity.[19] Thus, specific emphasis has been raised about what precautions must be taken against brain spyware.[89]

However, existing regulatory systems have not provided any special measures addressing newly growing risks facing neural data. Technically, there are no specific measures to ensure that applications and external services can access only to the neural information accepted by users, nor any limitation on manufacturers or third parties.[87] The Data Protection Impact Assessment (DPIA) under GDPR, though especially entailing measures for mitigating new technological risks, is still substantially a self-conducted process, subject to relatively weak supervision. Under the CCPA, businesses have obligations to maintain "reasonable" security procedures, but they apply generally to all personal information, with the "reasonable" standard being vague enough to limit its specificity. Even though the newly adopted Cyber Resilience Act of EU provides new security measures for digital products, it applies to such devices generally, without any specific measures addressing those special risks for neural data.[90]

Such regulatory gaps may leave ambiguity for some businesses to exploit in avoiding stricter security measures. In a review of privacy policies for certain BCI devices, research found that only a small part of the reviewed policies clearly provided encryption measures for limited types of data like biometric data (covering those for identifying purpose only). Most of such measures do not ensure that the encrypted data are inaccessible to the company and its employees, with the only exception of Apple promising that encrypted data are not accessible by its own employees.[5]

Ethics guidance and premarket review for consumer BCI devices

As BCI is a new generation of technology, relevant ethical considerations are still at their preliminary stage and have not encompassed comprehensive aspects of regulating such new techniques. Consequently, current regulatory approaches still lack specially designed ethical guidelines providing clear value basis. For example, while we note that neural data is "highly sensitive," it is still unsettled what are the further sensitivity differentiations for subcategories of neural data like those about emotions, cognition or behaviors. As a neuroscientist observed, there has been little "additional gradation" between non-sensitive data and sensitive data.[63] A regulatory system fully addressing special risks for neural data needs to have building foundations of ethical principles. As mentioned, ethics "shape laws."[32] The UNESCO Recommendation Draft also states that the ethics recommendation on neurotechnology provides a universal framework of values and principles to guide formulation of national legislation and policies.[30]

Furthermore, ethical reviews play a key role in research and clinical activities related to human subjects. For example, the US FDA has IRB review procedures in line with ethical standards respectively on human subject clinical investigations and premarket approval of medical devices.[91] However, such reviews usually only apply to activities or devices for clinical or medical activities. While medical devices are subject to heightened health data protections,[92] non-invasive BCIs not under medical context will be treated as consumer devices and face "almost no oversight."[2] With the increasing capabilities of educational or recreational BCIs for decoding and inferring from neural data, non-medical BCIs products should also be subject to certain premarket reviews.

International framework with legal effect

A special regulatory system for neural data is still at preliminary stage subject to debates.[57] Legislative progress just begins at tentative steps even at domestic law level, with only two states in the United States passing new laws. This indicates that it might be more difficult to achieve international frameworks with legal force. It has been consistently noticed that there are gaps in supranational and international law, with no mandatory governance framework focused on brain data currently existing,[8] and that there are currently no international frameworks that adequately protect against the risks posed by neurotechnologies.[93] The UNESCO Recommendation Draft is an important attempt at international level, yet targeting ethics rather than regulatory rules for data processing as a main subject.

Recommendations

Considering potential problems for regulating neural data processing, especially the remaining regulatory gaps, we propose that specific additional rules need to be introduced through further reform of current data laws. It may also take the form of an independent new type of special regulation with rules for data processing, like those for genetic information issues.[94]

Recommendation 1: Strengthen consent procedure enabling dynamic monitoring

Considering neural data as highly sensitive, a strengthened dynamic consent procedure is needed especially regarding repurposing and third-party sharing. First, heightened transparency for specified purposes should be ensured in a dynamic way enabling ongoing monitoring. There have been multiple proposals in this regard for "data literacy"[14] or "transparent view of how brain data is governed."[95]

Specifically, the Minnesota Neurodata Bill provides a reference by requiring an independent notice for "each time" connection to a BCI, covering types of potential uses and third parties with which data to be shared.[42] While the requirement of "each time" connection might be overly strict, it is suggested to add further purpose specification requirements for neural data in future data laws ensuring: (1) for the first time of collection, notice about all the planned types of uses of data in a detailed and item-by-item manner, as well as all third parties to be shared with for whatever grounds, listed in the same manner; (2) at any time the previous information has any changes (repurposing and new third parties), a new notice meeting the previous requirements. Particularly, the vague "incompatibility" standard under GDPR should be excluded from applicability at least to neural data in future data law reforms.

Second, the consent-giving procedure should also be administered dynamically at least for neural data. Granting consent should have a norm to revise consent over time to review unanticipated future use of the data.[7] Dynamic consent (DC) is not a new approach, while its mandatory application in data laws is the specific reform direction for neural data that we recommend. In its earlier stage, a DC has comprised the key element to enable individuals to turn consent decisions on and off "as easily as turning on a tap."[96] Based on the heightened transparency for purposes, the fundamental function of a DC should involve a requirement for separate consent/reconsent for any processing containing any changed purposes or third parties for data to be shared with (including international transfer). Further about the implementation model, there might be various methods to enforce DC requirements. Some key principles about the DC specially required for neural data may include: (1) there should be a mandatory real-time update for each connection of a BCI to its users to check whether there are any notices about changes in purposes or third parties, and such a notice should be displayed in a prominent manner; (2) in case of any such changes, there should be a real-time option for reconsent as condition for continuous use of the BCI device, displayed in a form different from initial consent for collection; (3) technically, the DC settings should allow users to consent to purposes and third parties on a sufficiently granular basis. Such functions should allow users to continuously renew and alter their consent preferences at any time, irrespective whether there have been changes to scope which they previously consented to.

Besides, a relevant key concern is the possible further classification of neural data, which might need to consider different degrees of sensitivity. As mentioned, "additional gradation" is still lacking. Certain subcategories of neural data might have extreme sensitivity such as those related to thoughts or behavior patterns, while others might be less sensitive such as general EEG data without inferences potential. The DC mechanism may need to have more special settings for the former type. However, the exact grading of detailed types of neural data is a complex and independent topic which needs further research in its special context.

Recommendation 2: Define and limit scope of research exception

Taking account of the differing approaches about research exception, it should be subject to policy concerns for each jurisdiction to decide whether or not to treat research as a listed exception to sensitive data processing. However, once research is provided as an exception for neural data, it should be inflicted with clear definition in a restrictive approach, favorably in an exhaustive or more illustrative manner and excluding research activities directly related to commercial purposes. There might be deviations for special research projects involving commercial elements and indeed conducive to public interest, notwithstanding an obligation to undergo ethical review by relevant expert committees.

In this regard, the CCPA's definition for research provides a valuable example, imposing limitative element like "public or scientific knowledge." Particularly, it incorporates "applicable ethics" as a dimension, where ethical principles may provide more detailed case-by-case standards for those complex research projects involving pioneering aspects of non-medical or commercial applications.

Recommendation 3: Enhance regulations for non-personal neural data

The sharing or cross-border transfer of certain types of non-personal neural data with special features should be subject to a security review procedure conducted by relevant data authorities. Such special non-personal neural data should at least cover those derived from certain data subject groups with shared characteristics (e.g., groups with a collective minority, ethnic, rare disease background), as well as those having the potential of being re-identified due to its special characteristics such as cognitive data. There has been regulatory proposal to include a legal prohibition on the use of inferences drawn from brain data in a way that could harm data subjects, including the reidentification of health data back to personal data.[80] It has also been proposed to establish review by project-specific or infrastructure-level data access review committees (DAC) for data requests about research on neuroimaging data including de-identified data.[97] Importantly, such special measures should not be limited to non-personal data held by public-sector bodies as regulated by the DGA, as relevant risks root in nature of such data themselves rather than their holders.

As for international transfer of such data, a catalogue for important/critical non-personal data (similar to that under China's PIPL) may be established under a regulatory system distinct from personal data laws.

Recommendation 4: Mandate additional cybersecurity measures

In response to security risks newly emerging or specially relevant to neural data, technical measures additional to current GDPR requirements should be mandated by data laws or relevant regulatory systems as privacy by design and by default for BCI devices. Firstly, "mandatory encryption" is necessary,[30] wherein enhanced encryption system should be required for any type of BCI device, whether for medical purposes or not. Robust methods may include homomorphic encryption,[98] secure multiparty computing[99] and differential privacy.[24]

Secondly, mandated measures should prevent anyone other than the user from access to neural data, including employees or technical contractors of the BCI operators, unless those who must have access due to performing tasks indispensable for the user's consented use for the BCI. As applicable, it is recommended to take edge-processing ensuring computing on local device rather than external servers or clouds, or to use end-to-end encryption.[5]

Thirdly, more BCI-responsive security frameworks against cyberattacks need to be introduced. The most discussed framework is distributed computation and decentralized data sharing.[100] Relevantly, studies also propose objective and verifiable blockchain tracking processing through federated learning rather than centralized processing.[97] Moreover, data perturbation is proposed to resist privacy attacks by randomly modifying original data or introducing noise to the dataset, and source-free transfer learning is suggested for privacy-preservation to eliminate the need for seeing the data from learning useful knowledge.[100] Further security measures may include a security lock-in between the EEG recording system and the processing system in order to avoid alteration or attack of the EEG signal during wireless transmission.[101]

In a more systematic way, scientists proposed the design of a Radio Frequency Identification (RFID) system, so as to identify brain activities in a secure real-time mode.[86] Some experts proposed a holistic security strategy involving elements of "Hide" (anonymization, privacy preserving machine learning and unlinking brain data from contextual data) and "separate" (local equipment) and "control" (no "always-on" BCIs).[102]

Recommendation 5: Establish premarket review procedure for BCI devices

In addition to existing ethical or special review for medical devices, a more comprehensive premarket review procedure needs to be established, further covering marketing of non-medical BCI devices as well as for BCI-R&D activities beyond clinical or research context. This may be a specific regulatory system better achieving the goals of the ordered measures in the Chilean supreme court decision[54]which is still vague and unstable on a case-by-case basis.

Such premarket review may center on assessing the data risks based on ethical guidance specially for neural data. The proposed DAC review committee introduced above is an exemplary approach, but is limited to neuroimaging data for research purpose only, not examining device functions either. The *Ethical Guideline for BCI Research* of China may also be an advisable model for regulatory approach, providing a mandatory data security review procedure for certain non-invasive BCI-related research which collects neural data, and imposing restrictions on neural data processing. But it is still limited to research activities and lack more specific rules on neural data sharing. Ideally, such an ethical review procedure may be broadened to cover premarket review for all types of BCI devices, applying ethical guidelines specially designed for neural data processing.

Recommendation 6: Promote international frameworks for universal ethics guidelines

Although it has been far from achieving an international treaty for legal rules on neural data, efforts for international frameworks of ethical principles have been developing. The OECD Recommendations made a meaningful preliminary attempt in this regard, and the UNESCO Recommendation Draft has made a further step in shaping a guideline with wide international consensus.

In line with these efforts, we recommend promoting international instruments through declarations or other soft laws specially for ethics principle of neural data protection or BCIs. These may take examples of prior achievements like the Universal Declaration on Bioethics and the Human Rights and International Declaration on Human Genetic Data,[e] which may provide value guidance and universally accepted basic principles for special protection of neural data.

Conclusion

This article provides elaboration on regulating neural data processing through data laws and relevant systems. Data laws may provide detailed and enforceable rules to regulate every stage of neural data use. In furtherance to human rights protection, whether traditional ones or new neurorights, data law approaches offer intricate balancing tools between competing interests of individual's privacy and public welfare related to health and scientific progress. Additional special rules should be established to address special challenges faced up by uniquely sensitive neural data. Reviewing current legal approaches, the GDPR model has been insufficient in this regard. The newest legislative reforms in CPA and CCPA made revolutionary attempts, but stopped at the "symbolic" incorporation of neural data, not stepping forward in introducing specific rules. The Minnesota Neurodata Bill is a more advanced approach and a worth-noting trend, yet still limited to few aspects of notice and consent.

Specific recommendations are made in this article for reforming relevant regulatory systems, suggesting newly designed data law approaches such as dynamic consent mechanism. Considering the sudden and unpredictable development style of BCI and AI, it is not over-vigilant or hasty to design precautionary special rules for regulating neural data processing in advance, as well as to promote relevant discussions, debates, and practices.

Limitations

In reviewing relevant legal approaches in regulatory practices, this article only selected a limited number of typical data laws and rules such as the GDPR of EU, the PIPL of China, and data laws or bills of certain states in the United States. The first constitutional case in Chile was also briefly compared but not the main concern of this research. Due to the fast development of relevant legislative reforms and various forms of data privacy legislations, there might be other legislations or cases particularly relevant to neural data which are not discussed in this article. Besides, the issue of BCI-generated neural data closely involves rapidly developing technical advancement and scientific studies, while this article may not cover the latest findings from scientific and technological fields of BCIs.

Acknowledgments: We thank the two anonymous reviewers for very helpful feedback and advice.

Declaration of conflicting interests: The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding: The authors are funded by the China National Social Sciences Fund Project, No.22BFX210 and supported by the Fundamental Research Funds for the Central Universities (22120240585).

ORCID iD: Hong Yang https://orcid.org/0009-0008-8824-6617
Li Jiang https://orcid.org/0000-0002-9094-0551

Notes

a. The Colorado House Bill 24-1058, April 17, 2024, Sec.1; The California SB 1223, September 28, 2024, Sec.1.5. The two amendments will be discussed further in Part IV.

b. Nick Statt. *Kernel is Trying to Hack the Human Brain—But Neuroscience has a Long Way to Go*, https://www.theverge.com/2017/2/22/14631122/kernel-neuroscience-bryan-johnson-human-intelligence-ai-startup, (2017, accessed 20 October 2024); Olivia Solon. *Facebook has 60 People Working on How to Read Your Mind*, https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8, (2017, accessed 20 October 2024).

c. https://www.neuroethicssociety.org/introduction (accessed 5 October 2024).

d. https://www.cohousedems.com/news/first-in-the-world-neural-data-protections-law-goes-into-effect, (accessed 10 November 2024).

e. https://www.unesco.org/en/legal-affairs/universal-declaration-bioethics-and-human-rights?hub=387 (accessed 1 November 2024); https://www.unesco.org/en/legal-affairs/international-declaration-human-genetic-data?hub=387 (accessed 1 November 2024).

References

1. Capitol Technology University. Neuralink's brain chip: how it works and what it means. Available at: https://www.captechu.edu/blog/neuralinks-brain-chip-how-it-works-and-what-it-means (2024, accessed 20 October 2024).
2. Genser J, Damianos S and Yuste R. Safeguarding brain data: assessing the privacy practices of consumer neurotechnology companies. NeuroRights Foundation, 2024.
3. International Bioethics Committee of UNESCO. Ethical issues of neurotechnology-report adopted in December 2021. UNESCO, 2022.
4. OECD. Recommendation on innovation in neurotechnology, OECD/Legal/0457, 11 December 2019.
5. Magee P, Ienca M and Farahany N. Beyond neural data: cognitive biometrics and mental privacy. *Neuron* 2024; 112: 3017–3028.
6. Jwa AS and Poldrack RA. Addressing privacy risk in neuroscience data: from data protection to harm prevention. *J Law Biosci* 2022; 9: lsac025.
7. Goering S, Klein E, Specker Sullivan L, et al. Recommendations for responsible development and application of neurotechnologies. *Neuroethics* 2021; 14: 365–386.
8. Ienca M, Fins JJ, Jox RJ, et al. Towards a governance framework for brain data. *Neuroethics* 2022; 15: 20.
9. Farahany NA. *The battle for your brain*. New York: St. Martin's Griffin, 2023, pp.46–56.
10. Spino J. Brain data availability presents unique privacy challenges. *AJOB Neurosci* 2024; 15: 146–148.
11. Brazal A, Pesce F, Beltrán M, et al. *TechDispatch on neurodata*. EDPS, Project Number: 2024.2368, 2024.
12. Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
13. Liv N and Greenbaum D. Integrating mental privacy within data protection laws: addressing the complexities of neurotechnology and the interdependence of human rights. *AJOB Neurosci* 2024; 15: 151–153.
14. Rainey S, McGillivray K, Akintoye S, et al. Is the European data protection regulation sufficient to deal with emerging data concerns relating to neurotechnology? *J Law Biosci* 2020; 7: lsaa051.

15. Sun X and Ye B. The functional differentiation of brain–computer interfaces (BCIs) and its ethical implications. *Humanit Soc Sci Commun* 2023; 10: 878.
16. Poldrack RA. Inferring mental states from neuroimaging data: from reverse inference to large-scale decoding. *Neuron* 2011; 72: 692–697.
17. Drew L. The ethics of brain-computer interfaces. *Nature* 2019; 571: S19–S21.
18. Lange J, Massart C, Mouraux A, et al. Side-channel attacks against the human brain: the PIN code case study (extended version). *Brain Inform* 2018; 5: 12.
19. Bernal SL, Celdran AH, Maimo LF, et al. Cyberattacks on miniature brain implants to disrupt spontaneous neural signaling. *IEEE Access* 2020; 8: 152204–152222.
20. Lenca M and Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sci Soc Policy* 2017; 13: 5.
21. Abel Wajnerman P. Is your neural data part of your mind? Exploring the conceptual basis of mental privacy. *Minds Mach* 2022; 32: 395–415.
22. Amadio J, Bi G-Q, Boshears PF, et al. Neuroethics questions to guide ethical research in the international brain initiatives. *Neuron* 2018; 100: 19–36.
23. New York City Bar Committee on Science and Law. Are your thoughts your own? Neuroprivacy and the legal implications of brain imaging. Available at: https://www.nycbar.org/pdf/report/Neuroprivacy-revisions.pdf (2005, accessed October 20, 2024).
24. Yuste R, Goering S, Arcas B, et al. Four ethical priorities for neurotechnologies and AI. *Nature* 2017; 551: 159–163.
25. Parens E and Johnston J. Does it make sense to speak of neuroethics? *EMBO Rep* 2007; 8: 61–64.
26. Hamilton J. If they could read your mind. *Stanford Magazine*. Available at: https://stanfordmag.org/contents/if-they-could-read-your-mind (2004, accessed October 31 2024).
27. O'Sullivan S, Chneiweiss H, Pierucci A, et al. Rapporteur report: neurotechnologies and human rights framework: do we need new human rights? Council of Europe and OECD, 2021.
28. Ochang P, Stahl BC and Eke D. The ethical and legal landscape of brain data governance. *PLoS One* 2022; 17: e0273473.
29. Vincent J-D. *Ethics and neurosciences*. Paris: International Bioethics Committee of UNESCO, 1995.
30. Outcome Document of the First Meeting of the AHEG-First Draft of a Recommendation on the Ethics of Neurotechnology (First Version), SHS/Bio/AHEG-Neuro/2024/1.REV, 9 May 2024.
31. Postan E. Narrative devices: neurotechnologies, information, and self-constitution. *Neuroethics* 2021; 14: 231–251.
32. Ochang P, Eke D and Stahl BC. Perceptions on the ethical and legal principles that influence global brain data governance. *Neuroethics* 2024; 17: 23.
33. Matthews D. Time is running out to regulate neurotechnology. *Science Business*. Available at: https://sciencebusiness.net/news/time-running-out-regulate-neurotechnology (9 December 2021, accessed 31 October 2024).
34. Judgement of the Court (Second Chamber), Case C-434/16, 20 December 2017.
35. Judgement of the Court (Second Chamber), Case C-582/14, 19 October, 2016.
36. EDPS. *The history of the general data protection regulation*. Available at: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (accessed 1 November 2024).
37. The Personal Information Protection Law of People's Republic of China, adopted in 2021.
38. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R Parts 160, 162, 164.
39. The California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2022 (CPRA), and further amended in 2024.
40. Colorado House Bill HB 24-1058 Concerning Protecting the Privacy of Individuals' Biological Data, and, in Connection Therewith, Protecting the Privacy of Neural Data and Expanding the Scope of the "Colorado Privacy Act" Accordingly, 2024.
41. California Senate Bill SB 1223: Consumer privacy: sensitive personal information: neural data (2023-2024).
42. Minnesota Bill SF 1110 for an act relating to data privacy; establishing neurodata rights; modifying certain crimes to add neurodata elements; providing civil and criminal penalties; amending Minnesota Statutes 2022, sections 13.04, by adding a subdivision; 609.88, subdivision 2; 609.891, subdivision 3; proposing coding for new law in Minnesota Statutes, chapter 325E. (2023-2024).
43. Ethical Guideline for BCI Research, National Committee of Scientific and Technological Ethics, Ministry of Science and Technology of PR. China, 2003.
44. USFDA. Implanted Brain-Computer Interface (BCI) Devices for Patients with Paralysis or Amputation Non-clinical Testing and Clinical Considerations: Guidance for Industry and Food and Drug Administration Staff; Docket No. FDA-2014-N-1130. 2021.
45. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, OJ L, 12.7.2024.
46. Chander A, Kaminski ME and Mc Geveran W. Catalyzing privacy law. *Minn Law Rev* 2021; 105: 1733–1803.
47. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, OJ L 152, 3.6.2022.
48. Proposal for a regulation of the European parliament and of the council on the European Health Data Space, COM(2022) 197 final.
49. Data Security Law of the People's Republic of China, adopted 10 June 2021, Art.21, 31.
50. Provisions on Administration of Security of Automobile Data. Order No.7 by Cyberspace Administration of China, etc. Available at: https://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm (accessed 15 October 2024).
51. Ordinance for Administration of Network Security, State Council Order No.790, 24 September 2024, Art. 37.

52. IBM, Greenberg J, Ringrose K, et al. *Privacy and connected mind: understanding the data flows and privacy risks of brain-computer interfaces*. Available at: https://fpf.org/wp-content/uploads/2021/11/FPF-BCI-Report-Final.pdf (accessed 31 August 2024).
53. Cornejo-Plaza MI, Cippitani R and Pasquino V. Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata. *Front Psychol* 2024; 15: 1330439.
54. Muñoz JM, Marinaro JÁ, Iglesias JA, et al. Effects of the first successful lawsuit against a consumer neurotechnology company for violating brain data privacy. *Nat Biotechnol* 2024; 42: 1015–1016.
55. Hertz N. Neurorights – do we need new human rights? A reconsideration of the right to freedom of thought. *Neuroethics* 2023; 16: 5.
56. Brazal A, Pesce F, Beltrán M, et al. TechDispatch on Neurodata, EDPS Project Number: 2024.2368, 2024.
57. Susser D and Cabrera LY. Brain data in context: are new rights the way to mental and brain privacy? *A JOB Neurosci* 2023; 15: 122–133.
58. Straczkiewicz M, James P and Onnela J-P. A systematic review of smartphone-based human activity recognition methods for health research. *NPJ Digit Med* 2021; 4: 148.
59. Lang M, McKibbin K, Shabani M, et al. Crowdsourcing smartphone data for biomedical research: ethical and legal questions. *Digit Health* 2023; 9: 1–5.
60. Botes M. Perspective chapter: making space for neuro rights in the context of brain-computer interfaces: one small step for human rights, one giant leap for mankind. In: Kashou NH (ed) *New insights in brain-computer interface systems*. Intechopen, 2023. Available at: https://www.intechopen.com/chapters/88036 (accessed 15 October 2024).
61. Kellmeyer P. Big brain data: on the responsible use of brain data from clinical and consumer-directed neurotechnological devices. *Neuroethics* 2021; 14: 83–98.
62. Elliott D. Data protection is more than privacy. *Eur Data Prot Law Rev* 2019; 5: 13–16.
63. Yuste R. Advocating for neurodata privacy and neurotechnology regulation. *Nat Protoc* 2023; 18: 2869–2875.
64. EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (version 1.1), adopted on 4 May 2020, para.156.
65. Becker R, Chokoshvili D, Thorogood A, et al. Purpose definition as a crucial step for determining the legal basis under the GDPR: implications for scientific research. *J Law Biosci* 2024; 11: lsae001.
66. Yusifova L. *Ethical and legal aspects of using brain computer interface in medicine: protection of patient's neuro privacy*. Doctoral Dissertation, Università di Bologna, 2020.
67. Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.5.2014.
68. EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b), adopted on 23 January 2019, para. 31.
69. Staunton C. Individual rights in biobank research under the GDPR. In: Slokenberga S, Tzortzatou O and Reichel J (eds) *GDPR And biobanking: individual rights, public interest and research regulation across Europe*. Switzerland: Springer, 2022, pp.91–104.
70. Jackson FLC. Tuskegee experiment. In: Mitcham C (ed) *Encyclopedia of science, technology and ethics*. USA: Macmillan Reference, 2005.
71. Judgment of the Court (Grand Chamber) of 18 October 2011, Oliver Brüstle v Greenpeace eV., para.46.
72. Jwa AS. *Summary of webinar on brain data governance and neurorights*. International Neuroethics Society. Available at: https://www.neuroethicssociety.org/webinar-data-2021 (2021, accessed 1 September 2024).
73. Salerno J, Knoppers BM, Lee LM, et al. Ethics, big data and computing in epidemiology and public health. *Ann Epidemiol* 2017; 27: 297–301.
74. Poldrack R and Gorgolewski K. Making big data open: data sharing in neuroimaging. *Nat Neurosci* 2014; 17: 1510–1517.
75. Hendriks S, Ramos KM and Grady C. Survey of investigators about sharing human research data in the neurosciences. *Neurology* 2022; 99: e1314–e1325.
76. Ienca M. *Common human rights challenges raised by different applications of neurotechnologies in the biomedical field*. EU: Council of Europe, 2021.
77. Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for federated learning on user-held data. *arXiv:1611.04482 [cs, stat]*. 2016.
78. Article 29 Data Pritection Working Group. Guidelines on the right to data portability, revised on 5 April 2017, WP 242 rev.01.
79. Judgement of the Court (Third Chamber), YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, Joined Cases C-141/12 and C-372/12, 17 July 2014.
80. Jwa AS and Martinez-Martin N. Rationales and approaches to protecting brain data: a scoping review. *Neuroethics* 2024; 17: 2.
81. Minssen T, Rajam N and Bogers M. Clinical trial data transparency and GDPR compliance: implications for data sharing and open innovation. *Sci Public Policy* 2021; 47: 616–626.
82. Pagallo U, Durante M, Monteleone S. What is new with the Internet of Things in privacy and data protection? Four legal challenges on sharing and control in IoT. In: Leenes R, Brakel Rv, Gutwirth S, etal (eds) *Data protection and privacy: (in)visibilities and infrastructures*. Switzerland: Springer, 2017, pp.59–78.
83. Staunton C, Shabani M, Mascalzoni D, et al. Ethical and social reflections on the proposed European Health Data Space. *Eur J Hum Genet* 2024; 32: 498–505.
84. Xynogalas V and Leiser (Mark) MR. The Metaverse: searching for compliance with the general data protection regulation. *Int Data Priv Law* 2024; 14: 89–105.
85. Rommelfanger KS, Pustilnik A and Salles A. Mind the gap: lessons learned from neurorights. Sci Diplom 2022.
86. Ajrawi S, Rao R and Sarkar M. Cybersecurity in brain-computer interfaces: RFID-based design-theoretical framework. *Inform Med Unlocked* 2021; 22: 100489.
87. Bernal SL, Celdrán AH, Pérez GM, et al. Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges. *ACM Comput Surv* 2022; 54: 1–35.
88. Bernal SL, Celdrán AH and Pérez GM. Eight reasons to prioritize brain-computer interface cybersecurity. *Commun ACM* 2023; 66: 68–78.

89. Ebers M. Regulating AI and robotics: ethical and legal challenges. In: Ebers M and Navas S (eds) *Algorithms and law*. New York: Cambridge University Press, 2020, p.53.
90. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) NO 168/2013 and (EU) 2019/1020 and DIRECTIVE (EU) 2020/1828, OJ L 2847, 20.11.2024.
91. C.F.R §46.109, 2018.
92. Wexler A and Reiner P. Oversight of direct-to-consumer neurotechnologies. *Science* 2019; 363: 234–235.
93. Genser J, Herrmann S and Yuste R. *International human rights protection gaps in the age of neurotechnology*. Neurorights Foundation. Available at: https://neurorightsfoundation.org/reports (2022, accessed 30 October 2024).
94. Ienca M and Malgieri G. Mental data protection and the GDPR. *J Law Biosci* 2022; 9: lsac006.
95. Price WN 2nd and Cohen IG. Privacy in the age of medical big data. *Nat Med* 2019; 25: 37–43.
96. Teare HJA, Prictor M and Kaye J. Reflections on dynamic consent in biomedical research: the story so far. *Eur J Hum Genet* 2021; 29: 649–656.
97. Eke DO, Bernard A, Bjaalie JG, et al. International data governance for neuroscience. *NEURON* 2022; 110: 600–612.
98. Xia K, Duch W, Sun Y, et al. Privacy-preserving brain–computer interfaces: a systematic review. *IEEE Trans Comput Soc Syst* 2023; 10: 2312–2324.
99. Agarwal A, Dowsley R, McKinney ND, et al. Protecting privacy of users in brain-computer interface applications. *IEEE Trans Neural Syst Rehabil Eng* 2019; 27: 1546–1555.
100. Jiang X, Fan J, Zhu Z, et al. Cybersecurity in neural interfaces: survey and future trends. *Comput Biol Med* 2023; 167: 107604.
101. Bhalerao S, Ansari IA and Kumar A. Protection of BCI system via reversible watermarking of EEG signal. *Electron Lett* 2020; 56: 1389–1392.
102. Kapitonova M, Kellmeyer P, Vogt S, et al. A framework for preserving privacy and cybersecurity in brain-computer interfacing applications. *arXiv:2209.09653* 2022. DOI: 10.48550/arXiv.2209.09653.